EIROPAS PARLAMENTA UN PADOMES REGULA (ES) Nr. 910/2014

(2014. gada 23. jūlijs)

par elektronisko identifikāciju un uzticamības pakalpojumiem elektronisko darījumu veikšanai iekšējā tirgū un ar ko atceļ Direktīvu 1999/93/EK

EIROPAS PARLAMENTS UN EIROPAS SAVIENĪBAS PADOME,

ņemot vērā Līgumu par Eiropas Savienības darbību un jo īpaši tā 114. pantu,

ņemot vērā Eiropas Komisijas priekšlikumu,

pēc leģislatīvā akta projekta nosūtīšanas valstu parlamentiem,

ņemot vērā Eiropas Ekonomikas un sociālo lietu komitejas atzinumu ([1]),

saskaņā ar parasto likumdošanas procedūru ([2]),

tā kā:

(1) Ļoti svarīgs ekonomiskās un sociālās izaugsmes faktors ir uzticēšanās tiešsaistes videi. Uzticēšanās trūkums, jo īpaši tad, ja tas rodas šķietama juridiskās noteiktības trūkuma dēļ, liek patērētājiem, uzņēmumiem un publiskām iestādēm vilcināties veikt darījumus elektroniski un pieņemt jaunus pakalpojumus.

(2) Šīs regulas mērķis ir stiprināt elektronisko darījumu uzticamību iekšējā tirgū, nodrošinot vienotu pamatu drošai elektroniskai mijiedarbībai starp iedzīvotājiem, uzņēmumiem, un publiskām iestādēm, tādējādi palielinot publisko un privāto tiešsaistes pakalpojumu, elektroniskās darījumdarbības un elektroniskās komercijas efektivitāti Savienībā.

(3) Eiropas Parlamenta un Padomes Direktīva 1999/93/EK ([3]) attiecās tikai uz elektroniskajiem parakstiem, nenodrošinot visaptverošu pārrobežu un starpnozaru regulējumu drošiem, uzticamiem un viegli lietojamiem elektroniskiem darījumiem. Ar šo regulu tiek stiprināts un paplašināts minētās direktīvas *acquis*.

(4) Komisijas 2010. gada 26. augusta paziņojumā "Digitālā programma Eiropai" tika konstatēts, ka galvenie šķēršļi, kas traucē izveidot digitālās ekonomikas noslēgto loku, ir digitālā tirgus sadrumstalotība, sadarbspējas trūkums un kibernoziedzības pieaugums. Arī 2010. gada ziņojumā par ES pilsonību "Likvidējot šķēršļus ES pilsoņu tiesību īstenošanai" Komisija uzsvēra, ka ir jāatrisina galvenās problēmas, kas Savienības pilsoņiem liedz izmantot digitālā vienotā tirgus un pārrobežu digitālo pakalpojumu sniegtos labumus.

(5) 2011. gada 4. februāra un 2011. gada 23. oktobra secinājumos Eiropadome Komisiju aicināja līdz 2015. gadam izveidot digitālo vienoto tirgu, panākt strauju progresu galvenajās digitālās ekonomikas jomās un veicināt pilnīgi integrētu digitālo vienoto tirgu, atvieglojot tiešsaistes pakalpojumu pārrobežu izmantošanu un īpašu uzmanību pievēršot drošas elektroniskās identifikācijas un autentifikācijas veicināšanai.

([1]) OV C 351, 15.11.2012., 73. lpp.
([2]) Eiropas Parlamenta 2014. gada 3. aprīļa nostāja (*Oficiālajā Vēstnesī* vēl nav publicēta) un Padomes 2014. gada 23. jūlija lēmums.
([3]) Eiropas Parlamenta un Padomes Direktīva 1999/93/EK (1999. gada 13. decembris) par Kopienas elektronisko parakstu sistēmu (OV L 13, 19.1.2000., 12. lpp.).

(6) Padome 2011. gada 27. maija secinājumos aicināja Komisiju sniegt ieguldījumu digitālā vienotā tirgus izveidē, radot piemērotus apstākļus tādu svarīgāko katalizatoru savstarpējai pārrobežu atzīšanai kā elektroniskā identifikācija, elektroniski dokumenti, elektroniski paraksti un elektroniski piegādes pakalpojumi, kā arī piemērotus apstākļus e-pārvaldes pakalpojumu sadarbspējai visā Eiropas Savienībā.

(7) Eiropas Parlaments 2010. gada 21. septembra rezolūcijā par iekšējā tirgus izveidi elektroniskās komercijas jomā ([1]) uzsvēra, cik nozīmīga ir elektronisko pakalpojumu drošība, īpaši elektronisko parakstu drošība, un ka nepieciešams izveidot publiskās atslēgas infrastruktūru visā Eiropā, un aicināja Komisiju izveidot Eiropas validācijas iestāžu vārteju, lai nodrošinātu elektronisko parakstu savstarpēju izmantojamību starpvalstu līmenī un palielinātu internetā veikto darījumu drošību.

(8) Eiropas Parlamenta un Padomes Direktīvā 2006/123/EK ([2]) noteikts, ka dalībvalstīm jāizveido vienoti kontaktpunkti (VP), lai ar attiecīgā VP starpniecību visas procedūras un formalitātes, kas ir saistītas ar piekļuvi pakalpojumu sniegšanas darbībai un ar tās veikšanu, ar attiecīgajām iestādēm varētu viegli veikt no attāluma un elektroniskā veidā. Daudziem tiešsaistes pakalpojumiem, kas pieejami ar VP starpniecību, ir vajadzīga elektroniskā identifikācija, autentifikācija un elektroniskais paraksts.

(9) Lielākajā daļā gadījumu iedzīvotāji nevar izmantot savu elektronisko identifikāciju, lai autentificētos citā dalībvalstī, jo viņu valsts elektroniskās identifikācijas shēmas nav atzītas citās dalībvalstīs. Minētais šķērslis elektronisko sistēmu jomā liedz pakalpojumu sniedzējiem pilnībā izmantot iekšējā tirgus labumus. Savstarpēji atzīti elektroniskās identifikācijas līdzekļi atvieglos daudzu pakalpojumu pārrobežu sniegšanu iekšējā tirgū un dos iespēju uzņēmumiem veikt pārrobežu darbību, neliekot pārvarēt daudzus šķēršļus saskarē ar publiskām iestādēm.

(10) Ar Eiropas Parlamenta un Padomes Direktīvu 2011/24/ES ([3]) izveidoja to valsts iestāžu tīklu, kuras ir atbildīgas par e-veselību. Lai palielinātu pārrobežu veselības aprūpes drošību un nepārtrauktību, šim tīklam ir jāizstrādā pamatnostādnes par elektronisku veselības aprūpes datu un pakalpojumu pārrobežu pieejamību, tostarp atbalstot "kopīgus identifikācijas un autentifikācijas pasākumus, lai veicinātu datu nodošanu pārrobežu veselības aprūpē". Elektroniskās identifikācijas un autentifikācijas savstarpējai atzīšanai ir būtiska nozīme, lai pārrobežu veselības aprūpe Eiropas iedzīvotājiem kļūtu par realitāti. Kad iedzīvotāji ārstēšanās nolūkā dodas uz citu valsti, viņu medicīniskajiem datiem ir jābūt pieejamiem valstī, kur notiek ārstēšanās. Tam ir jāizveido stabila, droša un uzticama elektroniskās identifikācijas sistēma.

(11) Šī regula būtu jāpiemēro, pilnībā ievērojot personas datu aizsardzības principus, kas noteikti Eiropas Parlamenta un Padomes Direktīvā 95/46/EK ([4]). Šajā sakarā, ņemot vērā savstarpējas atzīšanas principu, kas noteikts ar šo regulu, tiešsaistes pakalpojuma autentifikācijai būtu jāattiecas tikai uz tādu identifikācijas datu apstrādi, kas ir pienācīgi, atbilstīgi un nav pārmērīgi, lai tiešsaistē piešķirtu piekļuvi minētajam pakalpojumam. Arī uzticamības pakalpojumu sniedzējiem un uzraudzības iestādēm būtu jāievēro prasības, kas Direktīvā 95/46/EK ir noteiktas attiecībā uz apstrādes konfidencialitāti un drošību.

(12) Viens no šīs regulas mērķiem ir likvidēt šķēršļus, kas patlaban kavē to elektroniskās identifikācijas līdzekļu pārrobežu izmantošanu, kuri tiek lietoti dalībvalstīs, lai autentificētos vismaz sabiedriskajiem pakalpojumiem. Šīs regulas mērķis nav iejaukties dalībvalstīs jau izveidotajās elektroniskās identitātes pārvaldības sistēmās un ar to saistītās infrastruktūrās. Šīs regulas mērķis ir nodrošināt to, ka ar drošu elektronisko identifikāciju un autentifikāciju ir iespējams piekļūt dalībvalstu piedāvātajiem pārrobežu tiešsaistes pakalpojumiem.

([1]) OV C 50 E, 21.2.2012., 1. lpp.
([2]) Eiropas Parlamenta un Padomes Direktīva 2006/123/EK (2006. gada 12. decembris) par pakalpojumiem iekšējā tirgū (OV L 376, 27.12.2006., 36. lpp.).
([3]) Eiropas Parlamenta un Padomes Direktīva 2011/24/ES (2011. gada 9. marts) par pacientu tiesību piemērošanu pārrobežu veselības aprūpē (OV L 88, 4.4.2011., 45. lpp.).
([4]) Eiropas Parlamenta un Padomes Direktīva 95/46/EK (1995. gada 24. oktobris) par personu aizsardzību attiecībā uz personas datu apstrādi un šādu datu brīvu apriti (OV L 281, 23.11.1995., 31. lpp.).

(13) Dalībvalstīm arī turpmāk vajadzētu būt iespējai izvēlēties to, kādus līdzekļus izmantot vai ieviest elektroniskās identifikācijas nolūkiem, lai piekļūtu tiešsaistes pakalpojumiem. Tām arī vajadzētu būt iespējai izlemt, vai minēto līdzekļu nodrošināšanā iesaistīt privāto sektoru. Dalībvalstīm nevajadzētu būt pienākumam paziņot Komisijai par savām elektroniskās identifikācijas shēmām. Dalībvalstis pašas var izvēlēties, vai paziņot Komisijai par visām vai dažām, vai neziņot ne par vienu no tām elektroniskās identifikācijas shēmām, kas valsts līmenī tiek izmantotas, lai piekļūtu vismaz tiešsaistes sabiedriskajiem pakalpojumiem vai kādiem konkrētiem pakalpojumiem.

(14) Šajā regulā ir jāparedz daži nosacījumi attiecībā uz to, kuri elektroniskās identifikācijas līdzekļi ir jāatzīst un kā būtu jāpaziņo par elektroniskās identifikācijas shēmām. Minētajiem nosacījumiem būtu dalībvalstīm jāpalīdz veidot nepieciešamo uzticēšanos pārējo dalībvalstu elektroniskās identifikācijas shēmām un savstarpēji atzīt tos elektroniskās identifikācijas līdzekļus, kuri ietverti valstu paziņotajās shēmās. Savstarpējās atzīšanas princips būtu jāpiemēro, ja paziņotājas dalībvalsts elektroniskās identifikācijas shēmā ir izpildīti paziņošanas nosacījumi un paziņojums ir publicēts *Eiropas Savienības Oficiālajā Vēstnesī*. Tomēr savstarpējās atzīšanas principam būtu jāattiecas tikai uz autentificēšanos tiešsaistes pakalpojumam. Tam, kāda ir piekļuve minētajiem tiešsaistes pakalpojumiem un to galīgā piegāde pieprasītājam, vajadzētu būt cieši saistītam ar tiesībām saņemt šādus pakalpojumus saskaņā ar valsts tiesību aktos paredzētajiem nosacījumiem.

(15) Pienākumam atzīt elektroniskās identifikācijas līdzekļus būtu jāattiecas tikai uz tiem līdzekļiem, kuru identitātes uzticamības līmenis ir vienāds ar līmeni, kāds nepieciešams konkrētajam tiešsaistes pakalpojumam, vai ir augstāks. Turklāt minētais pienākums būtu jāpiemēro tikai tad, ja konkrētā publiskā iestāde izmanto tādu uzticamības līmeni, kas attiecībā uz piekļuvi minētajam pakalpojumam tiešsaistē, ir "būtisks" vai "augsts". Saskaņā ar Savienības tiesību aktiem dalībvalstīm arī turpmāk vajadzētu būt iespējai atzīt tādus elektroniskās identifikācijas līdzekļus, kuriem ir zemāks identitātes uzticamības līmenis.

(16) Uzticamības līmeņiem būtu jāraksturo elektroniskās identifikācijas līdzekļu ticamības pakāpe personas identitātes noskaidrošanā, tādējādi nodrošinot pārliecību, ka persona, kas uzdodas par personu ar kādu konkrētu identitāti, patiešām ir tā persona, kurai minētā identitāte ir piešķirta. Uzticamības līmenis ir atkarīgs no ticamības pakāpes, ko elektroniskās identifikācijas līdzekļi nodrošina attiecībā uz personas uzdoto vai piedāvāto identitāti, ņemot vērā procesus (piemēram, identitātes pierādīšanu un verifikāciju, un autentifikāciju), pārvaldības darbības (piemēram, vienību, kura izsniedz elektroniskās identifikācijas līdzekļus un šādu līdzekļu izsniegšanas procedūru) un ieviesto tehnisko kontroli. Pastāv dažādas uzticamības līmeņu tehniskās definīcijas un apraksti, kas izstrādāti Savienības finansētos liela mēroga izmēģinājuma projektos, standartizācijas un starptautiskās darbībās. Konkrēti, liela mēroga izmēģinājuma projekts *STORK* un ISO 29115 cita starpā atsaucas uz 2., 3. un 4. līmeni, kas būtu vislielākajā mērā jāņem vērā, nosakot minimālās tehniskās prasības, standartus un procedūras zemam, būtiskam un augstam uzticamības līmenim šīs regulas nozīmē, vienlaikus nodrošinot konsekventu šīs regulas piemērošanu, jo īpaši attiecībā uz augstu uzticamības līmeni saistībā ar identitātes pierādīšanu, lai izsniegtu kvalificētus sertifikātus. Izstrādātajām prasībām vajadzētu būt tehnoloģiju ziņā neitrālām. Vajadzīgās drošības prasības būtu jāspēj nodrošināt ar dažādu tehnoloģiju palīdzību.

(17) Dalībvalstīm būtu jāmudina privātais sektors brīvprātīgi izmantot paziņotajā shēmā ietvertos elektroniskās identifikācijas līdzekļus identificēšanas nolūkos, kad tas nepieciešams tiešsaistes pakalpojumiem vai elektroniskajiem darījumiem. Iespēja izmantot šādus elektroniskās identifikācijas līdzekļus privātajam sektoram dotu iespēju paļauties uz elektronisko identifikāciju un autentifikāciju, ko jau tagad daudzās dalībvalstīs plaši izmanto vismaz sabiedrisko pakalpojumu jomā, un šāda iespēja uzņēmumiem un iedzīvotājiem atvieglotu piekļuvi saviem tiešsaistes pakalpojumiem citās valstīs. Lai privātajam sektoram būtu vieglāk šādus elektroniskās identifikācijas līdzekļus izmantot citās valstīs, jebkuras dalībvalsts nodrošinātajai autentifikācijas iespējai vajadzētu būt pieejamai tām privātā sektora atkarīgajām pusēm, kas veic uzņēmējdarbību ārpus minētās dalībvalsts teritorijas, saskaņā ar tādiem pašiem nosacījumiem, kādus piemēro privātā sektora atkarīgajām pusēm, kas veic uzņēmējdarbību minētajā dalībvalstī. Tāpēc attiecībā uz privātā sektora atkarīgajām pusēm paziņotāja dalībvalsts var definēt noteikumus, kas attiecas uz piekļuvi autentifikācijas līdzekļiem. Šādos piekļuves noteikumos var būt sniegta informācija par to, vai ar paziņoto shēmu saistītie autentifikācijas līdzekļi privātā sektora atkarīgajām pusēm patlaban ir pieejami.

(18) Šajā regulā būtu jāparedz paziņotājas dalībvalsts, elektroniskās identifikācijas līdzekļus izsniedzošās personas un autentifikācijas procedūru veicošās personas atbildība par šajā regulā noteikto attiecīgo pienākumu neizpildi. Tomēr šī regula būtu jāpiemēro saskaņā ar valstu noteikumiem par atbildību. Tāpēc tā neietekmē, piemēram, valsts noteikumus par zaudējumu definīciju vai attiecīgajiem piemērojamiem procesuālajiem noteikumiem, tostarp noteikumiem par pierādīšanas pienākumu.

(19) Elektroniskās identifikācijas shēmu drošībai ir būtiska nozīme elektronisko identifikācijas līdzekļu uzticamai savstarpējai atzīšanai dažādās valstīs. Šādā kontekstā dalībvalstīm būtu jāsadarbojas jautājumā par elektroniskās identifikācijas shēmu drošību un sadarbspēju Savienības līmenī. Kad vien attiecībā uz elektroniskās identifikācijas shēmām ir vajadzīgs, lai atkarīgās puses valsts līmenī lietotu kādu konkrētu aparatūru vai programmatūru, pārrobežu sadarbspējas nolūkā ir nepieciešams, lai minētās dalībvalstis nenoteiktu šādas prasības un attiecīgas izmaksas atkarīgajām pusēm, kas veic uzņēmējdarbību ārpus šo dalībvalstu teritorijas. Minētajā gadījumā saistībā ar sadarbspējas sistēmas darbību būtu jāapspriež un jāizstrādā atbilstīgi risinājumi. Tomēr nav iespējams izvairīties no tehniskām prasībām, kas izriet no valstu elektroniskās identifikācijas ierīcēm piemītošām specifikācijām un kas var ietekmēt šādu elektronisko līdzekļu (piemēram, viedkaršu) turētājus.

(20) Dalībvalstu sadarbībai būtu jāatvieglo paziņoto elektroniskās identifikācijas shēmu tehniskā sadarbspēja, lai sekmētu augsta līmeņa uzticamību un riska pakāpei atbilstošu drošību. Informācijas un paraugprakses apmaiņai dalībvalstu starpā ar mērķi panākt savstarpēju atzīšanu būtu jāpalīdz īstenot šādu sadarbību.

(21) Ar šo regulu būtu arī jāizveido vispārējs tiesiskais regulējums uzticamības pakalpojumu izmantošanai. Tomēr ar šo regulu nebūtu jānosaka vispārīgs pienākums šos pakalpojumus izmantot vai instalēt piekļuves punktu visiem esošajiem uzticamības pakalpojumiem. Jo īpaši šai regulai nebūtu jāattiecas uz tādu pakalpojumu sniegšanu, kurus izmanto vienīgi noteikts dalībnieku kopums slēgtās sistēmās, kas neskar trešās personas. Piemēram, šīs regulas prasības nebūtu jāpiemēro sistēmām, kas izveidotas uzņēmumos vai valsts pārvaldēs, lai pārvaldītu iekšējas procedūras, izmantojot uzticamības pakalpojumus. Vienīgi sabiedrībai sniegtiem uzticamības pakalpojumiem, kas skar trešās personas, būtu jāatbilst šajā regulā noteiktajām prasībām. Šai regulai nebūtu jāattiecas arī uz tiem aspektiem, kas ir saistīti ar līgumu slēgšanu vai citu juridisku saistību uzņemšanos un šādu līgumu vai saistību derīgumu, ja attiecībā uz to veidu prasības noteiktas valsts vai Savienības tiesību aktos. Turklāt tai nebūtu jāietekmē valstu formātam izvirzītās prasības, kas attiecas uz publiskiem reģistriem, jo īpaši komercreģistriem un zemes reģistriem.

(22) Lai veicinātu uzticamības pakalpojumu vispārēju pārrobežu izmantošanu, būtu jānodrošina iespēja tos izmantot kā pierādījumu tiesvedībā visās dalībvalstīs. Ja vien šajā regulā nav paredzēts citādi, uzticamības pakalpojumu juridiskais spēks ir jānosaka ar valsts tiesību aktiem.

(23) Ciktāl ar šo regulu tiek noteikts pienākums atzīt kādu uzticamības pakalpojumu, šādu uzticamības pakalpojumu var noraidīt tikai tādā gadījumā, ja pienākuma adresāts to nevar nolasīt vai verificēt tehnisku iemeslu dēļ, ko adresāts nespēj tieši kontrolēt. Tomēr minētajam pienākumam nebūtu jānozīmē tas, ka publiskai struktūrai ir jāiegādājas tāda aparatūra un programmatūra, lai tā varētu tehniski nolasīt visus esošos uzticamības pakalpojumus.

(24) Dalībvalstis, ievērojot Savienības tiesību aktus, var saglabāt vai ieviest valsts noteikumus attiecībā uz uzticamības pakalpojumiem, ja ar šo regulu veiktā saskaņošana attiecībā uz minētajiem pakalpojumiem nav pilnīga. Tomēr šīs regulas prasībām atbilstošiem uzticamības pakalpojumiem būtu jānodrošina brīva aprite iekšējā tirgū.

(25) Dalībvalstīm arī turpmāk vajadzētu būt iespējai noteikt citus uzticamības pakalpojumu veidus papildus tiem, kas minēti šajā regulā iekļautajā uzticamības pakalpojumu pilnīgajā sarakstā, lai valsts līmenī tos varētu atzīt par kvalificētiem uzticamības pakalpojumiem.

(26) Ņemot vērā tehnoloģiju attīstības ātrumu, šajā regulā būtu jāizmanto pieeja, kas paredz inovācijas iespēju.

(27) Šai regulai vajadzētu būt tehnoloģiju ziņā neitrālai. No tās izrietošajām juridiskajām sekām vajadzētu būt panākamām ar jebkuriem tehniskiem līdzekļiem ar noteikumu, ka tiek izpildītas šīs regulas prasības.

(28) Lai vairotu jo īpaši mazo un vidējo uzņēmumu (MVU) un patērētāju uzticēšanos iekšējam tirgum un veicinātu uzticamības pakalpojumu un produktu izmantošanu, būtu jāievieš jēdzieni "kvalificēti uzticamības pakalpojumi" un "kvalificēts uzticamības pakalpojumu sniedzējs", lai noteiktu prasības un pienākumus, kas garantē augsta līmeņa drošību attiecībā uz jebkuru sniegto kvalificēto uzticamības pakalpojumu un lietoto produktu.

(29) Atbilstīgi pienākumiem, kas noteikti ar Padomes Lēmumu 2010/48/EK ([1]) apstiprinātajā Apvienoto Nāciju Organizācijas Konvencijā par personu ar invaliditāti tiesībām, jo īpaši tās 9. pantā, personām ar invaliditāti vajadzētu būt iespējai izmantot uzticamības pakalpojumus un tiešo lietotāju produktus, kurus izmanto, sniedzot minētos pakalpojumus, ar tādiem pašiem nosacījumiem, kādi attiecas uz citiem patērētājiem. Tāpēc, ja iespējams, būtu jānodrošina, lai sniegtie uzticamības pakalpojumi un tiešo lietotāju produkti, ko izmanto minēto pakalpojumu sniegšanā, būtu pieejami personām ar invaliditāti. Pamatojuma izvērtējumā *inter alia* būtu jāietver tehniski un ekonomiski apsvērumi.

(30) Dalībvalstīm būtu jāizraugās uzraudzības iestāde vai uzraudzības iestādes šajā regulā minēto uzraudzības darbību veikšanai. Dalībvalstīm arī vajadzētu būt iespējai, savstarpēji vienojoties ar citu dalībvalsti, izlemt par uzraudzības iestādes izraudzīšanos minētās citas dalībvalsts teritorijā.

(31) Uzraudzības iestādēm būtu jāsadarbojas ar datu aizsardzības iestādēm, piemēram, informējot tās par kvalificēto uzticamības pakalpojumu sniedzēju revīzijas rezultātiem, ja šķiet, ka ir notikuši personas datu aizsardzības noteikumu pārkāpumi. Sniedzot informāciju, būtu jo īpaši jāietver drošības incidenti un personas datu pārkāpumi.

(32) Visiem uzticamības pakalpojumu sniedzējiem būtu jānosaka pienākums ievērot labu praksi drošības jomā, kas atbilst ar to darbību saistītajiem riskiem, lai tādējādi sekmētu lietotāju uzticēšanos vienotajam tirgum.

(33) Noteikumiem par pseidonīmu izmantošanu sertifikātos nebūtu jākavē dalībvalstis pieprasīt personu identifikāciju atbilstīgi Savienības vai valsts tiesību aktiem.

(34) Visām dalībvalstīm būtu jāievēro kopējas būtiskas uzraudzības prasības, lai kvalificētu uzticamības pakalpojumu jomā nodrošinātu līdzvērtīgu drošības līmeni. Lai visā Savienībā būtu vieglāk konsekventi piemērot minētās prasības, dalībvalstīm būtu jāpieņem salīdzināmas procedūras un jāapmainās ar informāciju par savu uzraudzības darbību un paraugpraksi šajā jomā.

(35) Visiem uzticamības pakalpojumu sniedzējiem būtu jāpiemēro šīs regulas prasības, jo īpaši drošības un atbildības jomā, lai nodrošinātu pienācīgu centību, pārredzamību un pārskatatbildību to darbībās un pakalpojumos. Tomēr, ņemot vērā uzticamības pakalpojumu sniedzēju sniegto pakalpojumu veidu, ir lietderīgi tiktāl, ciktāl tas attiecas uz minētajām prasībām, nošķirt kvalificētus un nekvalificētus uzticamības pakalpojumu sniedzējus.

(36) Uzraudzības režīma izveidošanai attiecībā uz visiem uzticamības pakalpojumu sniedzējiem būtu jānodrošina vienlīdzīgi konkurences apstākļi to darbību un pakalpojumu drošībai un atbildībai par tiem, tādējādi sekmējot lietotāju aizsardzību un iekšējā tirgus darbību. Nekvalificētiem uzticamības pakalpojumu sniedzējiem būtu jāpiemēro attiecīgas un reaģējošas *ex post* uzraudzības darbības, kuras attaisno to sniegto pakalpojumu un darbību būtība. Tāpēc uzraudzības iestādei nebūtu jānosaka vispārējs pienākums uzraudzīt nekvalificētus pakalpojumu sniedzējus. Uzraudzības iestādei būtu jārīkojas tikai tad, kad tā ir saņēmusi informāciju (piemēram, no paša nekvalificētā uzticamības pakalpojumu sniedzēja, citas uzraudzības iestādes, saņēmusi lietotāja vai darījumdarbības partnera paziņojumu vai uz pašas izmeklējumu pamata), ka nekvalificētais uzticamības pakalpojumu sniedzējs neievēro šajā regulā noteiktās prasības.

([1]) Padomes Lēmums 2010/48/EK (2009. gada 26. novembris) par to, lai Eiropas Kopiena noslēgtu Apvienoto Nāciju Organizācijas Konvenciju par personu ar invaliditāti tiesībām (OV L 23, 27.1.2010., 35. lpp.).

(37) Šajā regulā būtu jāparedz visu uzticamības pakalpojumu sniedzēju atbildība. Jo īpaši tajā ir noteikts atbildības režīms, saskaņā ar kuru visiem uzticamības pakalpojumu sniedzējiem vajadzētu būt atbildīgiem par zaudējumu, kas radīts jebkurai fiziskai vai juridiskai personai šajā regulā minēto pienākumu neizpildes dēļ. Lai vienkāršāk novērtētu finansiālo risku, kāds uzticamības pakalpojumu sniedzējiem iespējams būtu jāuzņemas vai kāds tiem būtu jāsedz ar apdrošināšanas polisēm, ar šo regulu uzticamības pakalpojumu sniedzējiem tiek ļauts ar konkrētiem nosacījumiem noteikt ierobežojumus to sniegto pakalpojumu izmantošanai, un nenest atbildību par zaudējumiem, kas rodas izmantojot pakalpojumus, kuri pārsniedz šādus ierobežojumus. Patērētāji būtu iepriekš pienācīgi jāinformē par ierobežojumiem. Minētajiem ierobežojumiem vajadzētu būt atpazīstamiem trešai personai, piemēram, informāciju par ierobežojumiem ietverot sniegtā pakalpojuma noteikumos vai izmantojot citus atpazīstamus līdzekļus. Lai īstenotu minētos principus, šī regula būtu jāpiemēro saskaņā ar valstu noteikumiem par atbildību. Tāpēc šī regula neietekmē valstu noteikumus, piemēram, par zaudējumu, nodoma vai nolaidības definīciju vai attiecīgajiem piemērojamiem procesuālajiem noteikumiem.

(38) Drošības pārkāpumu paziņošana un drošības risku izvērtēšana ir būtiski aspekti, kas drošības vai integritātes pārkāpumu gadījumā ļautu sniegt atbilstīgu informāciju attiecīgajām pusēm.

(39) Lai Komisija un dalībvalstis varētu novērtēt ar šo regulu ieviestā pārkāpumu paziņošanas mehānisma efektivitāti, būtu jānosaka, lai uzraudzības iestādes iesniegtu Komisijai un Eiropas Savienības Tīklu un informācijas drošības aģentūrai (*ENISA*) informatīvus kopsavilkumus.

(40) Lai Komisija un dalībvalstis varētu novērtēt ar šo regulu ieviestā pastiprinātas uzraudzības mehānisma efektivitāti, būtu jāpieprasa uzraudzības iestādēm iesniegt ziņojumus par savu darbību. Tas būtu lietderīgi, lai sekmētu labas prakses apmaiņu starp uzraudzības iestādēm, un nodrošinātu galveno uzraudzības prasību konsekventas un efektīvas īstenošanas pārbaudi visās dalībvalstīs.

(41) Lai nodrošinātu kvalificētu uzticamības pakalpojumu ilgtspējību un ilglaicīgumu un sekmētu lietotāju uzticēšanos kvalificētu uzticamības pakalpojumu nepārtrauktībai, uzraudzības iestādēm būtu jāpārliecinās, vai pastāv darbības pārtraukšanas plāni un vai noteikumi par pārtraukšanas plāniem tiek pareizi piemēroti, gadījumos, kad kvalificētie uzticamības pakalpojumu sniedzēji pārtrauc savas darbības.

(42) Dalībvalstīs būtu jāizveido uzraudzības iestāžu savstarpējas palīdzības sistēma, lai atvieglotu kvalificētu uzticamības pakalpojumu sniedzēju uzraudzību, piemēram, gadījumā, ja pakalpojumu sniedzējs pakalpojumus piedāvā citas dalībvalsts teritorijā un tur nav pakļauts uzraudzībai vai ja pakalpojumu sniedzēja datori atrodas citas dalībvalsts teritorijā, nevis tajā dalībvalstī, kurā minētais pakalpojumu sniedzējs veic uzņēmējdarbību.

(43) Lai nodrošinātu kvalificētu uzticamības pakalpojumu sniedzēju un to sniegto pakalpojumu atbilstību šīs regulas prasībām, atbilstības novērtēšanas struktūrai būtu jāveic atbilstības novērtēšana, un kvalificētiem uzticamības pakalpojumu sniedzējiem būtu iegūtie atbilstības novērtēšanas ziņojumi jāiesniedz uzraudzības iestādei. Kad vien uzraudzības iestāde pieprasa kvalificētam uzticamības pakalpojumu sniedzējam iesniegt *ad hoc* atbilstības novērtēšanas ziņojumu, uzraudzības iestādei būtu jo īpaši jāievēro labas pārvaldības principi, tostarp pienākums sniegt pamatojumu saviem lēmumiem, kā arī proporcionalitātes princips. Tāpēc uzraudzības iestādei būtu pienācīgi jāpamato lēmums pieprasīt *ad hoc* atbilstības novērtēšanu.

(44) Šīs regulas mērķis ir nodrošināt saskaņotu regulējumu, lai sniegtu augsta līmeņa drošību un juridisko noteiktību uzticamības pakalpojumiem. Šajā sakarā, risinot produktu un pakalpojumu atbilstības novērtēšanu, Komisijai attiecīgos gadījumos būtu jārod sinerģija ar esošajām attiecīgajām Eiropas un starptautiskajām sistēmām, piemēram, Eiropas Parlamenta un Padomes Regulu (EK) Nr. 765/2008 ([1]), kurā noteiktas atbilstības novērtēšanas struktūru akreditācijas un produktu tirgus uzraudzības prasības.

([1]) Eiropas Parlamenta un Padomes Regula (EK) Nr. 765/2008 (2008. gada 9. jūlijs), ar ko nosaka akreditācijas un tirgus uzraudzības prasības attiecībā uz produktu tirdzniecību un atceļ Regulu (EEK) Nr. 339/93 (OV L 218, 13.8.2008., 30. lpp.).

(45) Lai efektīvi noritētu ieviešanas process, kura rezultātā kvalificētos uzticamības pakalpojumu sniedzējus un to sniegtos kvalificētos uzticamības pakalpojumus iekļautu uzticamības sarakstos, būtu jāsekmē iepriekšēja apspriešanās starp kvalificētiem uzticamības pakalpojumu sniedzējiem un kompetento uzraudzības iestādi, tādējādi atvieglojot uzticamības pārbaudi, kas jāveic pirms kvalificētu uzticamības pakalpojumu sniegšanas.

(46) Uzticamības saraksti ir būtiski, lai panāktu uzticēšanos tirgus dalībnieku starpā, jo tajos norādīts pakalpojumu sniedzēja kvalifikācijas statuss uzraudzības laikā.

(47) Ticamība tiešsaistes pakalpojumiem un ērta to izmantošana ir būtiska, lai lietotāji pilnībā gūtu labumu no elektroniskajiem pakalpojumiem un apzināti uz tiem paļautos. Šajā nolūkā būtu jārada ES uzticamības marķējums, lai identificētu kvalificētus uzticamības pakalpojumus, ko sniedz kvalificēti uzticamības pakalpojumu sniedzēji. Šāds ES uzticamības marķējums kvalificētiem uzticamības pakalpojumiem skaidri atšķirtu kvalificētus uzticamības pakalpojumus no citiem uzticamības pakalpojumiem, tādējādi sekmējot pārredzamību tirgū. ES uzticamības marķējuma izmantošanai kvalificētiem uzticamības pakalpojumu sniedzējiem vajadzētu būt brīvprātīgai, un tai nebūtu jārada nekādas citas prasības papildu tām, kas ir paredzētas šajā regulā.

(48) Lai nodrošinātu elektronisko parakstu savstarpēju atzīšanu, drošības līmenim jābūt augstam, taču īpašos gadījumos, piemēram, saistībā ar Komisijas Lēmumu 2009/767/EK ([1]), būtu jāakceptē elektroniskie paraksti arī ar zemāku drošības nodrošinājuma līmeni.

(49) Ar šo regulu būtu jānosaka princips, ka elektroniskā paraksta juridisko spēku nebūtu jānoraida elektroniskā formāta dēļ vai tādēļ, ka tas neatbilst kvalificētā elektroniskā paraksta prasībām. Tomēr elektronisko parakstu juridiskais spēks ir jānosaka ar valsts tiesību aktiem, izņemot šajā regulā noteiktās prasības, proti, ka kvalificētiem elektroniskajiem parakstiem būtu jāpiešķir līdzvērtīgs juridiskais spēks kā parakstiem ar roku.

(50) Tā kā patlaban dalībvalstu kompetentās iestādes, savus dokumentus parakstot elektroniski, izmanto uzlabotu elektronisko parakstu dažādus formātus, ir jānodrošina, lai dalībvalstis spētu tehniski atbalstīt vismaz vairākus uzlabotu elektronisko parakstu formātus tad, kad tās saņem elektroniski parakstītus dokumentus. Tāpat, ja dalībvalstu kompetentās iestādes izmanto uzlabotus elektroniskos zīmogus, būtu jānodrošina, ka tās atbalstītu vismaz vairākus uzlabotu elektronisko zīmogu formātus.

(51) Parakstītājam būtu jāspēj uzticēt kvalificētas elektroniskā paraksta radīšanas ierīces trešās personas aprūpei ar noteikumu, ka tiek īstenoti pienācīgi mehānismi un procedūras, kas garantē, ka tikai parakstītājs kontrolē sava elektroniskā paraksta radīšanas datu izmantošanu, un ka saistībā ar ierīces izmantošanu ir izpildītas kvalificētā elektroniskā paraksta prasības.

(52) Aizvien biežāk notiek elektronisko parakstu attālināta izveide, proti, kad elektroniskais paraksts parakstītāja vārdā tiek izveidots vidē, ko pārvalda uzticamības pakalpojumu sniedzējs, jo tam ir daudzkārtējas ekonomiskas priekšrocības. Tomēr, lai nodrošinātu, ka šādi elektroniskie paraksti tiek juridiski atzīti tā pat kā tie elektroniskie paraksti, kas izveidoti vidē, kuru pilnībā pārvalda lietotājs, attālināta elektroniskā paraksta pakalpojuma sniedzējiem būtu jāpiemēro konkrētas drošības, pārvaldības un administratīvās procedūras, un jāizmanto uzticamas sistēmas un produkti, tostarp droši elektroniskie sakaru kanāli, ar mērķi garantēt elektroniskā paraksta izveides vides uzticamību un to, ka parakstītājs ir vienīgais, kurš kontrolē sava elektroniskā paraksta izveides vidi. Ja kvalificēts elektroniskais paraksts ir veidots ar attālināta elektroniskā paraksta izveides ierīci, būtu jāpiemēro prasības, kas saskaņā ar šo regulu ir piemērojamas kvalificētu uzticamības pakalpojumu sniedzējiem.

([1]) Komisijas Lēmums 2009/767/EK (2009. gada 16. oktobris) par pasākumiem, lai veicinātu procedūru veikšanu elektroniski, izmantojot vienotos kontaktpunktus atbilstoši Eiropas Parlamenta un Padomes Direktīvai 2006/123/EK par pakalpojumiem iekšējā tirgū (OV L 274, 20.10.2009., 36. lpp.).

(53) Kvalificēta sertifikāta apturēšana ir uzticamības pakalpojumu sniedzēju pieņemta darbības prakse vairākās dalībvalstīs, kura atšķiras no sertifikāta atsaukšanas un no kuras uz laiku izriet sertifikāta derīguma zudums. Juridiskās noteiktības dēļ vienmēr ir skaidri jānorāda sertifikāta apturēšanas statuss. Šajā nolūkā uzticamības pakalpojumu sniedzēji ir atbildīgi par to, lai skaidri norādītu sertifikāta statusu un, ja tas ir apturēts, precīzu laikposmu, uz kādu sertifikāts ir apturēts. Ar šo regulu uzticamības pakalpojumu sniedzējiem vai dalībvalstīm nebūtu jāuzliek par pienākumu izmantot apturēšanu, taču būtu jāparedz pārredzamības noteikumi, kad un kādos gadījumos šāda prakse ir pieejama.

(54) Kvalificētu sertifikātu pārrobežu sadarbspēja un atzīšana ir kvalificētu elektronisko parakstu atzīšanas priekšnosacījums. Tāpēc uz kvalificētiem sertifikātiem nebūtu jāattiecas nevienai obligātai prasībai, kas pārsniedz šajā regulā noteiktās prasības. Tomēr valstu līmenī būtu jāļauj kvalificētos sertifikātos iekļaut raksturīgās pazīmes, piemēram, unikālos identifikatorus, ar noteikumu, ka šādas raksturīgās pazīmes nekavē kvalificētu sertifikātu un elektronisko parakstu pārrobežu sadarbspēju un atzīšanu.

(55) IT drošības sertifikācija, kuras pamatā ir starptautiski standarti, piemēram, ISO 15408 un ar to saistītas novērtēšanas metodes un savstarpējās atzīšanas režīmi, ir būtisks instruments, lai verificētu kvalificēta elektroniskā paraksta radīšanas ierīču drošību, un tā būtu jāveicina. Tomēr inovatīviem risinājumiem un pakalpojumiem, piemēram, mobilajam parakstam un mākoņparakstam, ir nepieciešami kvalificēta elektroniskā paraksta radīšanas ierīču tehniski un organizatoriski risinājumi, kuriem drošības standarti iespējams vēl nav pieejami vai kuriem pašlaik notiek pirmā IT drošības sertifikācija. Šāda kvalificēta elektroniskā paraksta radīšanas ierīču drošības līmeni varētu novērtēt, izmantojot alternatīvus procesus, tikai tad, ja šādi drošības standarti nav pieejami, vai ja pašlaik notiek pirmā IT drošības sertifikācija. Minētajiem procesiem vajadzētu būt salīdzināmiem ar IT drošības sertifikācijas standartiem, ciktāl to drošības līmeņi ir līdzvērtīgi. Minētos procesus varētu sekmēt ar salīdzinošo izvērtēšanu.

(56) Šajā regulā būtu jāizklāsta prasības kvalificēta elektroniskā paraksta radīšanas ierīcēm, lai nodrošinātu uzlabotu elektronisko parakstu funkcionalitāti. Šī regula neaptver visu sistēmvidi, kurā šādas ierīces darbojas. Tāpēc kvalificētu paraksta radīšanas ierīču sertifikācijas jomā būtu jāietver tikai aparatūra un sistēmas programmatūra, ko izmanto, lai pārvaldītu un aizsargātu paraksta izveides datus, kas tiek radīti, uzglabāti vai apstrādāti paraksta radīšanas ierīcē. Kā precizēts attiecīgos standartos, no sertifikācijas pienākuma jomas nebūtu jāizslēdz paraksta radīšanas lietojumprogrammatūra.

(57) Lai nodrošinātu juridisko noteiktību attiecībā uz paraksta derīgumu, ir būtiski precizēt tos kvalificēta elektroniskā paraksta datus, kuri būtu jānovērtē atkarīgajai pusei, kura veic validāciju. Turklāt prasību precizēšana attiecībā uz tādiem kvalificētiem uzticamības pakalpojumu sniedzējiem, kas var sniegt kvalificētus validēšanas pakalpojumus atkarīgajām pusēm, kuras nevēlas vai nespēj pašas veikt kvalificētu elektronisko parakstu validāciju, būtu jāsekmē privātā un publiskā sektora ieguldījumi šādos pakalpojumos. Izpildot abus nosacījumus, kvalificēta elektroniskā paraksta validēšanai būtu jākļūst par vienkāršu un Savienības līmenī visām pusēm piemērotu procedūru.

(58) Ja, veicot darījumu, vajadzīgs juridiskas personas kvalificēts elektroniskais zīmogs, jāakceptē būtu arī juridiskās personas pilnvarotā pārstāvja kvalificēts elektroniskais paraksts.

(59) Elektroniskie zīmogi būtu jāizmanto kā pierādījums tam, ka elektronisko dokumentu izsniegusi juridiska persona, garantējot dokumenta izcelsmi un integritāti.

(60) Uzticamības pakalpojumu sniedzējiem, kas izsniedz kvalificētus elektronisko zīmogu sertifikātus, būtu jāievieš vajadzīgie pasākumi, lai varētu noskaidrot fiziskas personas identitāti, kas pārstāv juridisko personu, kurai tiek sniegts kvalificēts elektroniskā zīmoga sertifikāts, ja šāda identifikācija ir vajadzīga valsts līmenī saistībā ar tiesvedību vai administratīviem procesiem.

(61) Ar šo regulu būtu jānodrošina informācijas ilgtermiņa saglabāšana, lai nodrošinātu elektronisko parakstu un elektronisko zīmogu juridisko derīgumu ilgākos laikposmos un garantētu, ka tos var validēt neatkarīgi no turpmākas tehnoloģiju attīstības.

(62) Lai nodrošinātu kvalificētu elektronisko laika zīmogu drošību, šajā regulā būtu jānosaka prasība izmantot uzlabotu elektronisko zīmogu vai uzlabotu elektronisko parakstu vai citas līdzvērtīgas metodes. Paredzams, ka inovāciju rezultātā varētu tapt jaunas tehnoloģijas, kas varētu nodrošināt līdzvērtīgu drošības līmeni laika zīmogiem. Ja tiek izmantota cita metode, kas nav uzlabots elektroniskais zīmogs vai uzlabots elektroniskais paraksts, būtu jāatstāj kvalificētā uzticamības pakalpojumu sniedzēja ziņā, vai atbilstības novērtēšanas ziņojumā parādīt, ka šāda metode nodrošina līdzvērtīgu drošības līmeni un atbilst šajā regulā noteiktajiem pienākumiem.

(63) Elektroniskiem dokumentiem ir nozīme pārrobežu elektronisko darījumu turpmākai attīstībai iekšējā tirgū. Ar šo regulu būtu jānosaka princips, ka elektroniska dokumenta juridisko spēku nebūtu jānoraida elektroniskā formāta dēļ, lai nodrošinātu, ka elektronisku darījumu nenoraida tikai tādēļ, ka dokuments ir elektroniskā formātā.

(64) Izskatot uzlabotu elektronisko parakstu un zīmogu formātus, Komisijai būtu jābalstās uz esošo praksi, standartiem un tiesību aktiem, jo īpaši Komisijas Lēmumu 2011/130/ES [1].

(65) Elektroniskos zīmogus var izmantot ne vien juridiskas personas izsniegtu dokumentu autentificēšanai, bet arī visu juridiskas personas digitālo aktīvu, piemēram, programmatūru kodu vai serveru, autentificēšanai.

(66) Ir būtiski izveidot tiesisko regulējumu, lai veicinātu pārrobežu atzīšanu starp esošajām valstu tiesību sistēmām attiecībā uz elektroniski reģistrētiem piegādes pakalpojumiem. Minētais regulējums varētu arī radīt jaunas tirgus iespējas Savienības uzticamības pakalpojumu sniedzējiem piedāvāt jaunus elektroniski reģistrētus piegādes pakalpojumus visā Eiropā.

(67) Tīmekļa vietņu autentifikācijas pakalpojumi nodrošina veidu, kā tīmekļa vietnes apmeklētājs var būt drošs, ka par šo tīmekļa vietni atbild īsta un likumīga vienība. Minētie pakalpojumi palīdz veidot uzticēšanos un ticamību, veicot darījumdarbību tiešsaistē, jo lietotāji uzticēsies autentificētai tīmekļa vietnei. Tīmekļa vietņu autentifikācijas pakalpojumu sniegšana un izmantošana ir pilnīgi brīvprātīga. Tomēr, lai tīmekļa vietņu autentifikācija kļūtu par veidu, kā palielināt uzticēšanos, sniedzot labāku pieredzi lietotājam un turpmāku izaugsmi iekšējā tirgū, ar šo regulu būtu sniedzējiem un to sniegtajiem pakalpojumiem jānosaka minimālie drošības un atbildības pienākumi. Minētajā nolūkā vērā ir ņemti rezultāti, kas gūti nozares vadībā veiktajās iniciatīvās, piemēram, sertificēšanas iestāžu/pārlūku forums – CA/B forums. Turklāt šai regulai nebūtu jākavē citu veidu vai metožu izmantošana tīmekļa vietņu autentifikācijai, uz kuru šī regula neattiecas, un tai nebūtu jāliedz tīmekļa vietņu autentifikācijas pakalpojumu sniedzējiem no trešām valstīm sniegt to pakalpojumus Savienības klientiem. Tomēr būtu vajadzīgs, lai pakalpojumu sniedzējam no trešās valsts tīmekļa vietņu autentifikācijas pakalpojumi būtu atzīti par kvalificētiem pakalpojumiem saskaņā ar šo regulu tikai tad, ja ir noslēgts starptautisks nolīgums starp Savienību un valsti, kurā pakalpojumu sniedzējs veic uzņēmējdarbību.

(68) Saskaņā ar Līguma par Eiropas Savienības darbību (LESD) noteikumiem par uzņēmējdarbības veikšanu jēdziens "juridiskas personas" sniedz uzņēmējiem izvēles brīvību attiecībā uz juridisko formu, ko tie uzskata par piemērotu, lai veiktu savas darbības. Tādējādi "juridiskas personas" LESD nozīmē ir visas vienības, kas izveidotas atbilstīgi kādas dalībvalsts tiesību aktiem vai ko šie tiesību akti reglamentē, neatkarīgi no to juridiskās formas.

(69) Savienības iestādes, struktūras, birojus un aģentūras mudina atzīst elektronisko identifikāciju un uzticamības pakalpojumus, uz kuriem attiecas šī regula, lai aktīvāk izmantotu administratīvo sadarbību, jo īpaši attiecībā uz esošo labo praksi un rezultātiem, kas gūti patlaban īstenotajos projektos tajās jomās, uz kurām attiecas šī regula.

[1] Komisijas Lēmums 2011/130/ES (2011. gada 25. februāris), ar kuru nosaka minimālās prasības kompetento iestāžu elektroniski parakstītu dokumentu pārrobežu apstrādei saskaņā ar Eiropas Parlamenta un Padomes Direktīvu 2006/123/EK par pakalpojumiem iekšējā tirgū (OV L 53, 26.2.2011., 66. lpp.).

(70) Lai elastīgi un ātri papildinātu dažus šajā regulā precīzi noteiktus tehniskos aspektus, pilnvaras pieņemt aktus saskaņā ar LESD 290. pantu būtu jādeleģē Komisijai attiecībā uz kritērijiem, kas jāievēro par kvalificētu elektroniskā paraksta radīšanas ierīču sertifikāciju atbildīgām iestādēm. Ir īpaši būtiski, lai Komisija, veicot sagatavošanas darbus, rīkotu atbilstīgas apspriešanās, tostarp ekspertu līmenī. Komisijai, sagatavojot un izstrādājot deleģētos aktus, būtu jānodrošina vienlaicīga, savlaicīga un atbilstīga attiecīgo dokumentu nosūtīšana Eiropas Parlamentam un Padomei.

(71) Lai nodrošinātu vienādus nosacījumus šīs regulas īstenošanai, būtu jāpiešķir īstenošanas pilnvaras Komisijai, jo īpaši attiecībā uz to standartu identifikācijas numuru precizēšanu, kuru izmantošana ļautu izdarīt pieņēmumu par dažu šajā regulā noteikto prasību ievērošanu. Minētās pilnvaras būtu jāizmanto saskaņā ar Eiropas Parlamenta un Padomes Regulu (ES) Nr. 182/2011 ([1]).

(72) Pieņemot deleģētos vai īstenošanas aktus, Komisijai būtu pienācīgi jāņem vērā Eiropas un starptautisko standartizācijas organizāciju un struktūra, jo īpaši Eiropas Standartizācijas komitejas (*CEN*), Eiropas Telekomunikāciju standartu institūta (ETSI), Starptautiskās Standartizācijas organizācijas (*ISO*) un Starptautiskās Telesakaru savienības (*ITU*) izstrādātie standarti un tehniskās specifikācijas, lai nodrošinātu elektroniskās identifikācijas un uzticamības pakalpojumu augsta līmeņa drošību un sadarbspēju.

(73) Juridiskās noteiktības un skaidrības labad Direktīva 1999/93/EK būtu jāatceļ.

(74) Lai nodrošinātu juridisko noteiktību tiem tirgus dalībniekiem, kuri jau izmanto kvalificētus sertifikātus, kas izsniegti fiziskām personām saskaņā ar Direktīvu 1999/93/EK, ir jāparedz pietiekami ilgs pārejas laikposms. Līdzīgā veidā būtu jānosaka pārejas pasākumi drošām paraksta radīšanas ierīcēm, kuru atbilstība ir noteikta saskaņā ar Direktīvu 1999/93/EK, kā arī sertifikācijas pakalpojumu sniedzējiem, kas izsniedz kvalificētus sertifikātus pirms 2016. gada 1. jūlija. Visbeidzot, ir arī jānodrošina, lai Komisijai būtu līdzekļi, kas tai ļautu īstenošanas aktus un deleģētos aktus pieņemt pirms minētās dienas.

(75) Šajā regulā minētie piemērošanas datumi neskar esošos pienākumus, kas dalībvalstīm jau ir noteikti Savienības tiesību aktos, jo īpaši Direktīvā 2006/123/EK.

(76) Ņemot vērā to, ka šīs regulas mērķus nevar pietiekami labi sasniegt atsevišķās dalībvalstīs, bet rīcības mēroga dēļ tos var labāk sasniegt Savienības līmenī, Savienība var pieņemt pasākumus saskaņā ar Līguma par Eiropas Savienību 5. pantā noteikto subsidiaritātes principu. Saskaņā ar minētajā pantā noteikto proporcionalitātes principu šajā regulā paredz vienīgi tos pasākumus, kas ir vajadzīgi minēto mērķu sasniegšanai.

(77) Saskaņā ar Eiropas Parlamenta un Padomes Regulas (EK) Nr. 45/2001 ([2]) 28. panta 2. punktu ir notikusi apspriešanās ar Eiropas Datu aizsardzības uzraudzītāju, kas 2012. gada 27. septembrī sniedza atzinumu ([3]),

([1]) Eiropas Parlamenta un Padomes Regula (ES) Nr. 182/2011 (2011. gada 16. februāris), ar ko nosaka normas un vispārīgus principus par dalībvalstu kontroles mehānismiem, kuri attiecas uz Komisijas īstenošanas pilnvaru izmantošanu (OV L 55, 28.2.2011., 13. lpp.).

([2]) Eiropas Parlamenta un Padomes Regula (EK) Nr. 45/2001 (2000. gada 18. decembris) par fizisku personu aizsardzību attiecībā uz personas datu apstrādi Kopienas iestādēs un struktūrās un par šādu datu brīvu apriti (OV L 8, 12.1.2001., 1. lpp.).

([3]) OV C 28, 30.1.2013., 6. lpp.

IR PIEŅĒMUŠI ŠO REGULU.

I NODAĻA

VISPĀRĪGI NOTEIKUMI

1. pants

Priekšmets

Lai nodrošinātu iekšējā tirgus pienācīgu darbību, vienlaikus cenšoties panākt elektroniskās identifikācijas līdzekļu un uzticamības pakalpojumu pienācīgu drošības līmeni, šajā regulā:

a) tiek izklāstīti nosacījumi, saskaņā ar kuriem dalībvalstis atzīst fizisku un juridisku personu elektroniskās identifikācijas līdzekļus, kuri ietverti citas dalībvalsts paziņotajā elektroniskās identifikācijas shēmā;

b) tiek izklāstīti noteikumi par uzticamības pakalpojumiem, jo īpaši attiecībā uz elektroniskiem darījumiem; un

c) tiek izveidots tiesiskais regulējums attiecībā uz elektroniskajiem parakstiem, elektroniskajiem zīmogiem, elektroniskajiem laika zīmogiem, elektroniskajiem dokumentiem, elektroniski reģistrētiem piegādes pakalpojumiem un sertifikācijas pakalpojumiem tīmekļa vietņu autentifikācijai.

2. pants

Darbības joma

1. Šo regulu piemēro elektroniskās identifikācijas shēmām, par kurām ir paziņojušas dalībvalstis, un uzticamības pakalpojumu sniedzējiem, kas veic uzņēmējdarbību Savienībā.

2. Šo regulu nepiemēro tādu uzticamības pakalpojumu sniegšanai, kurus izmanto vienīgi slēgtās sistēmās, kas izriet no valsts tiesību aktiem vai nolīgumiem starp noteiktu dalībnieku kopumu.

3. Šī regula neskar valstu vai Savienības tiesību aktus, kas saistīti ar līgumu slēgšanu un derīgumu vai citu juridisku vai procesuālu saistību uzņemšanos attiecībā uz formātu.

3. pants

Definīcijas

Šajā regulā izmanto šādas definīcijas:

1) "elektroniskā identifikācija" ir tādu elektronisku personas identifikācijas datu izmantošanas process, kas unikālā veidā apliecina fiziskās vai juridiskās personas identitāti vai tādas fiziskas personas identitāti, kas pārstāv juridisku personu;

2) "elektroniskās identifikācijas līdzekļi" ir materiāli un/vai nemateriāli elementi, kas ietver personas identifikācijas datus un ko izmanto, lai autentificētos tiešsaistes pakalpojumam;

3) "personas identifikācijas dati" ir datu kopums, kas ļauj noskaidrot fiziskas vai juridiskas personas identitāti, vai tādas fiziskas personas identitāti, kas pārstāv juridisku personu;

4) "elektroniskās identifikācijas shēma" ir elektroniskās identifikācijas sistēma, kurā elektroniskās identifikācijas līdzekļus izsniedz fiziskām vai juridiskām personām vai tādām fiziskām personām, kas pārstāv juridiskas personas;

5) "autentifikācija" ir elektronisks process, kas dara iespējamu fiziskas vai juridiskas personas elektronisko identifikāciju vai elektronisko datu izcelsmes un integritātes apstiprināšanu;

6) "atkarīgā puse" ir fiziska vai juridiska persona, kas paļaujas uz elektronisku identifikāciju vai uzticamības pakalpojumu;

7) "publiskā iestāde" ir valsts, reģionāla vai pašvaldības iestāde, publisko tiesību subjekts vai apvienība, ko veido viena vai vairākas šādas iestādes vai viens vai vairāki šādi publisko tiesību subjekti, vai privāta vienība, ko pilnvarojusi vismaz viena no minētajām iestādēm, subjektiem vai apvienībām, lai sniegtu publiskus pakalpojumus, darbojoties saskaņā ar šādu pilnvarojumu;

8) "publisko tiesību subjekts" ir struktūra, kas definēta Eiropas Parlamenta un Padomes Direktīvas 2014/24/ES ([1]) 2. panta 1. punkta 4. apakšpunktā;

9) "parakstītājs" ir fiziska persona, kura rada elektronisku parakstu;

10) "elektroniskais paraksts" ir elektroniski dati, kas pievienoti citiem elektroniskajiem datiem vai loģiski saistīti ar tiem un ko parakstītājs izmanto, lai parakstītos;

11) "uzlabots elektroniskais paraksts" ir elektronisks paraksts, kas atbilst 26. pantā izklāstītajām prasībām;

12) "kvalificēts elektroniskais paraksts" ir uzlabots elektroniskais paraksts, kas radīts ar kvalificētu elektroniskā paraksta radīšanas ierīci, pamatojoties uz kvalificētu elektroniskā paraksta sertifikātu;

13) "elektroniskā paraksta radīšanas dati" ir unikāli dati, ko parakstītājs izmanto elektroniska paraksta radīšanai;

14) "elektroniskā paraksta sertifikāts" ir elektronisks apliecinājums, kas saista elektroniskā paraksta validācijas datus ar fizisku personu un apliecina vismaz minētās personas vārdu vai pseidonīmu;

15) "kvalificēts elektroniskā paraksta sertifikāts" ir elektroniskā paraksta sertifikāts, ko izsniedz kvalificēts uzticamības pakalpojumu sniedzējs un kas atbilst I pielikumā noteiktajām prasībām;

16) "uzticamības pakalpojums" ir elektronisks pakalpojums, parasti par atlīdzību, kas ietver:

a) elektronisko parakstu, elektronisko zīmogu vai elektronisko laika zīmogu, elektroniski reģistrētu piegādes pakalpojumu un ar minētajiem pakalpojumiem saistītu sertifikātu radīšanu, verifikāciju un validāciju; vai

b) tīmekļa vietņu autentifikācijas sertifikātu radīšanu, verifikāciju un validāciju; vai

c) ar minētajiem pakalpojumiem saistītu elektronisko parakstu, zīmogu vai sertifikātu saglabāšanu;

17) "kvalificēts uzticamības pakalpojums" ir uzticamības pakalpojums, kas atbilst šajā regulā noteiktajām piemērojamām prasībām;

([1]) Eiropas Parlamenta un Padomes Direktīva 2014/24/ES (2014. gada 26. februāris) par publisko iepirkumu un ar ko atceļ Direktīvu 2004/18/EK (OV L 94, 28.3.2014., 65. lpp.).

18) "atbilstības novērtēšanas struktūra" ir Regulas (EK) Nr. 765/2008 2. panta 13. punktā definēta struktūra, kas saskaņā ar minēto regulu ir akreditēta kā kompetenta veikt kvalificēta uzticamības pakalpojumu sniedzēja un tā sniegtu kvalificētu uzticamības pakalpojumu atbilstības novērtējumu;

19) "uzticamības pakalpojumu sniedzējs" ir fiziska vai juridiska persona, kas sniedz vienu vai vairākus uzticamības pakalpojumus vai nu kā kvalificēti, vai kā nekvalificēti uzticamības pakalpojumu sniedzēji;

20) "kvalificēts uzticamības pakalpojumu sniedzējs" ir uzticamības pakalpojumu sniedzējs, kas sniedz vienu vai vairākus kvalificētus uzticamības pakalpojumus un kuram uzraudzības iestāde ir piešķīrusi kvalificētā statusu;

21) "produkts" ir aparatūra vai programmatūra, vai aparatūras vai programmatūras attiecīgas sastāvdaļas, ko paredzēts izmantot uzticamības pakalpojumu sniegšanai;

22) "elektroniskā paraksta radīšanas ierīce" ir konfigurēta programmatūra vai aparatūra, ko izmanto elektroniska paraksta radīšanai;

23) "kvalificēta elektroniskā paraksta radīšanas ierīce" ir elektroniskā paraksta radīšanas ierīce, kas atbilst II pielikumā noteiktajām prasībām;

24) "zīmoga radītājs" ir juridiska persona, kas rada elektronisku zīmogu;

25) "elektroniskais zīmogs" ir elektroniski dati, kas pievienoti citiem elektroniskajiem datiem vai loģiski saistīti ar tiem, lai garantētu šo pēdējo izcelsmi un integritāti;

26) "uzlabots elektroniskais zīmogs" ir elektronisks zīmogs, kas atbilst 36. pantā izklāstītajām prasībām;

27) "kvalificēts elektroniskais zīmogs" ir uzlabots elektroniskais zīmogs, kas radīts ar kvalificētu elektroniskā zīmoga radīšanas ierīci un kura pamatā ir kvalificēts elektroniskā zīmoga sertifikāts;

28) "elektroniskā zīmoga radīšanas dati" ir unikāli dati, ko elektroniskā zīmoga radītājs izmanto elektroniska zīmoga radīšanai;

29) "elektroniskā zīmoga sertifikāts" ir elektronisks apliecinājums, kas saista elektroniskā zīmoga validācijas datus ar juridisku personu un apliecina minētās personas nosaukumu;

30) "kvalificēts elektroniskā zīmoga sertifikāts" ir elektroniskā zīmoga sertifikāts, ko izsniedz kvalificēts uzticamības pakalpojumu sniedzējs un kas atbilst III pielikumā noteiktajām prasībām;

31) "elektroniskā zīmoga radīšanas ierīce" ir konfigurēta programmatūra vai aparatūra, ko izmanto elektroniska zīmoga radīšanai;

32) "kvalificēta elektroniskā zīmoga radīšanas ierīce" ir elektroniskā zīmoga radīšanas ierīce, kas *mutatis mutandis* atbilst II pielikumā noteiktajām prasībām;

33) "elektroniskais laika zīmogs" ir elektroniski dati, kas saista citus elektroniskos datus ar konkrētu laiku, apstiprinot šo pēdējo esamību minētajā laikā;

34) "kvalificēts elektroniskais laika zīmogs" ir elektroniskais laika zīmogs, kas atbilst 42. pantā noteiktajām prasībām;

35) "elektronisks dokuments" ir jebkāds saturs, kas tiek glabāts elektroniskā formātā, jo īpaši teksta vai skaņas, vizuāls vai audiovizuāls ieraksts;

36) "elektroniski reģistrēts piegādes pakalpojums" ir pakalpojums, kuru izmantojot, ar elektroniskiem līdzekļiem tiek nosūtīti dati starp trešām personām, sniedzot apliecinājumu par nosūtīto datu apstrādi, tostarp pierādījumu par datu nosūtīšanu un saņemšanu, un kuri nodrošina nosūtīto datu aizsardzību pret pazušanu, zādzību vai jebkādu neatļautu sagrozīšanu;

37) "kvalificēts elektroniski reģistrēts piegādes pakalpojums" ir elektroniski reģistrēts piegādes pakalpojums, kas atbilst 44. pantā noteiktajām prasībām;

38) "tīmekļa vietņu autentifikācijas sertifikāts" ir apliecinājums, kas ļauj autentificēt tīmekļa vietni un saista tīmekļa vietni ar fizisko vai juridisko personu, kurai sertifikāts ir izsniegts;

39) "kvalificēts tīmekļa vietņu autentifikācijas sertifikāts" ir tīmekļa vietņu autentifikācijas sertifikāts, ko izsniedz kvalificēts uzticamības pakalpojumu sniedzējs un kas atbilst IV pielikumā noteiktajām prasībām;

40) "validācijas dati" ir dati, ko izmanto elektroniska paraksta vai elektroniska zīmoga validācijai;

41) "validācija" ir elektroniskā paraksta vai zīmoga verifikācija un apstiprināšana, ka tas ir derīgs.

4. pants

Iekšējā tirgus principi

1. Netiek ierobežota tādu uzticamības pakalpojumu sniegšanu kādā dalībvalstī, ko nodrošina citā dalībvalstī reģistrēts uzticamības pakalpojumu sniedzējs tādu iemeslu dēļ, kas izriet no jomām, uz ko attiecas šī regula.

2. Produktus un uzticamības pakalpojumus, kas atbilst šai regulai, var laist brīvā apritē iekšējā tirgū.

5. pants

Datu apstrāde un aizsardzība

1. Personas datus apstrādā saskaņā ar Direktīvu 95/46/EK.

2. Neskarot juridisko spēku, kas atbilstīgi valsts tiesību aktiem ir pseidonīmiem, pseidonīmu izmantošana elektroniskos darījumos nav aizliegta.

II NODAĻA

ELEKTRONISKĀ IDENTIFIKĀCIJA

6. pants

Savstarpējā atzīšana

1. Ja saskaņā ar valsts tiesību aktiem vai administratīvo praksi tāda pakalpojuma piekļuvei, ko publiskā iestāde tiešsaistē sniedz vienā dalībvalstī, ir nepieciešama elektroniskā identifikācija, izmantojot elektroniskās identifikācijas līdzekļus, tad elektroniskās identifikācijas līdzekļi, kuri izsniegti citā dalībvalstī tiek atzīti pirmajā dalībvalstī, lai veiktu minētā tiešsaistes pakalpojuma pārrobežu autentifikāciju, ar noteikumu, ka tiek ievēroti šādi nosacījumi:

a) elektroniskās identifikācijas līdzekļus izsniedz saskaņā ar elektroniskās identifikācijas shēmu, kas iekļauta atbilstīgi 9. pantam Komisijas publicētā sarakstā;

b) elektroniskās identifikācijas līdzekļu uzticamības līmenis atbilst tādam uzticamības līmenim, kas ir līdzvērtīgs vai lielāks par uzticamības līmeni, kādu noteikusi attiecīgā publiskā iestāde attiecībā uz piekļuvi tiešsaistes pakalpojumam pirmajā dalībvalstī, ar noteikumu, ka minēto elektroniskās identifikācijas līdzekļu uzticamības līmenis atbilst būtiskam vai augstam uzticamības līmenim;

c) attiecīgā publiskā iestāde izmanto būtisku vai augstu uzticamības līmeni attiecībā uz piekļuvi minētajam pakalpojumam tiešsaistē.

Šāda atzīšana notiek vēlākais 12 mēnešus pēc tam, kad Komisija publicē pirmās daļas a) apakšpunktā minēto sarakstu.

2. Elektroniskās identifikācijas līdzekļus, kas izsniegti saskaņā ar elektroniskās identifikācijas shēmu, kura ir iekļauta atbilstīgi 9. pantam Komisijas publicētā sarakstā un kura atbilst zemam uzticamības līmenim, publiskās iestādes var atzīt, lai minētās iestādes veiktu tiešsaistē sniegta pakalpojuma pārrobežu autentifikāciju.

7. pants

Elektroniskās identifikācijas shēmu atbilstība paziņošanai

Par elektroniskās identifikācijas shēmu var paziņot saskaņā ar 9. panta 1. punktu ar noteikumu, ka ir izpildīti visi šie nosacījumi:

a) elektroniskās identifikācijas līdzekļus saskaņā ar elektroniskās identifikācijas shēmu izsniedz:

i) paziņotāja dalībvalsts;

ii) atbilstīgi paziņotājas dalībvalsts pilnvarai; vai

iii) neatkarīgi no paziņotājas dalībvalsts, un tos atzīst minētā dalībvalsts;

b) elektroniskās identifikācijas līdzekļus saskaņā ar elektroniskās identifikācijas shēmu var izmantot, lai būtu pieejams vismaz viens pakaplojums, ko sniedz publiskā iestāde un saistībā ar ko paziņotājā dalībvalstī jāizmanto elektroniskā identifikācija;

c) elektroniskās identifikācijas shēma un saskaņā ar to izsniegtie elektroniskās identifikācijas līdzekļi atbilst vismaz viena uzticamības līmeņa, kas ir izklāstīts 8. panta 3. punktā minētajā īstenošanas aktā, prasībām;

d) paziņotāja dalībvalsts nodrošina, ka, izsniedzot elektroniskās identifikācijas līdzekļus saskaņā ar minēto shēmu, 3. panta 1. punktā minētajai fiziskai vai juridiskai personai saskaņā ar 8. panta 3. punktā minētā īstenošanas aktā izklāstītā attiecīgā uzticamības līmeņa tehniskajām specifikācijām, standartiem un procedūrām tiek piešķirti personas identifikācijas dati, kas unikāli apliecina attiecīgo personu;

e) puse, kas izsniedz elektroniskās identifikācijas līdzekļus saskaņā ar minēto shēmu, nodrošina, ka elektroniskās identifikācijas līdzekļus piešķir šā panta d) punktā minētajai personai atbilstīgi 8. panta 3. punktā minētajā īstenošanas aktā izklāstītā attiecīgā uzticamības līmeņa tehniskajām specifikācijām, standartiem un procedūrām;

f) paziņotāja dalībvalsts nodrošina, ka ir pieejama autentifikācija tiešsaistē, lai ikviena atkarīgā puse, kas veic uzņēmējdarbību citas dalībvalsts teritorijā, spēj apstiprināt elektroniskā formātā saņemtos personas identifikācijas datus.

Attiecībā uz atkarīgajām pusēm, kas nav publiskās iestādes, paziņotāja dalībvalsts var definēt noteikumus, kas attiecas uz piekļuvi minētajai autentifikācijai. Pārrobežu autentifikāciju sniedz bez maksas, kad to veic saistībā ar publiskās iestādes sniegtu tiešsaistes pakalpojumu.

Dalībvalstis neizvirza nekādas īpašas nesamērīgas tehniskas prasības tām atkarīgajām pusēm, kas plāno veikt šādu autentifikāciju, ja šādas prasības neļauj īstenot vai būtiski kavē paziņoto elektroniskās identifikācijas shēmu sadarbspēju;

g) vismaz sešus mēnešus pirms paziņošanas saskaņā ar 9. panta 1. punktu paziņotāja dalībvalsts sakarā ar 12. panta 5. punktā noteikto pienākumu citām dalībvalstīm sniedz minētās shēmas aprakstu atbilstīgi 12. panta 7. punktā minētajos īsenošanas aktos noteiktajai procesuālajai kārtībai;

h) elektroniskās identifikācijas shēma atbilst prasībām, kas izklāstītas 12. panta 8. punktā minētajā īstenošanas aktā.

8. pants

Elektroniskās identifikācijas shēmu uzticamības līmeņi

1. Elektroniskās identifikācijas shēmā, kas paziņota saskaņā ar 9. panta 1. punktu, precizē atbilstīgi minētajai shēmai izsniegto elektroniskās identifikācijas līdzekļu zemo, būtisko un/vai augsto uzticamības līmeni.

2. Zemais, būtiskais un augstais uzticamības līmenis atbilst attiecīgi šādiem kritērijiem:

a) zems uzticamības līmenis attiecas uz elektroniskās identifikācijas līdzekļiem saistībā ar elektroniskās identifikācijas shēmu, kas sniedz ierobežotu ticamības pakāpi attiecībā uz personas apgalvotu vai paustu identitāti, un to raksturo atsauce uz tehniskajām specifikācijām, standartiem un procedūrām, kas ir ar to saistītas, tostarp tehnisko kontroli, kuru mērķis ir mazināt identitātes nepareizas izmantošanas vai izmainīšanas risku;

b) būtisks uzticamības līmenis attiecas uz elektroniskās identifikācijas līdzekļiem saistībā ar elektroniskās identifikācijas shēmu, kas sniedz būtisku ticamības pakāpi attiecībā uz personas apgalvotu vai paustu identitāti, un to raksturo atsauce uz tehniskajām specifikācijām, standartiem un procedūrām, kas ir ar to saistītas, tostarp tehnisko kontroli, kuru mērķis ir būtiski mazināt identitātes nepareizas izmantošanas vai izmainīšanas risku;

c) augsts uzticamības līmenis attiecas uz elektroniskās identifikācijas līdzekļiem saistībā ar elektroniskās identifikācijas shēmu, kas sniedz augstāku ticamības pakāpi attiecībā uz personas apgalvotu vai paustu identitāti nekā būtisks uzticamības līmenis, un to raksturo atsauce uz tehniskajām specifikācijām, standartiem un procedūrām, kas ir ar to saistītas, tostarp tehnisko kontroli, kuru mērķis ir novērst identitātes nepareizu izmantošanu vai izmainīšanu.

3. Līdz 2015. gada 18. septembrim, ņemot vērā attiecīgos starptautiskos standartus un ievērojot 2. punktu, Komisija ar īstenošanas aktiem nosaka minimālās tehniskās specifikācijas, standartus un procedūras, uz kuriem atsaucoties 1. punkta nolūkā ir noteikts elektroniskās identifikācijas līdzekļu zems, būtisks un augsts uzticamības līmenis.

Minētās minimālās tehniskās specifikācijas, standartus un procedūras nosaka, atsaucoties uz šādu turpmāk minētu elementu uzticamību un kvalitāti:

a) procedūra, ar kuru pierāda un verificē to fizisko vai juridisko personu identitāti, kas iesniedz pieteikumu elektroniskās identifikācijas līdzekļu izsniegšanai;

b) procedūra, ar kuru izsniedz pieprasītos elektroniskās identifikācijas līdzekļus;

c) autentifikācijas mehānisms, ar kuru fiziskā vai juridiskā persona izmanto elektroniskās identifikācijas līdzekļus, lai apstiprinātu savu identitāti atkarīgajai pusei;

d) vienība, kas izsniedz elektroniskās identifikācijas līdzekļus;

e) jebkura cita struktūra, kas ir iesaistīta pieteikuma iesniegšanā attiecībā uz elektroniskās identifikācijas līdzekļiem; un

f) izsniegto elektroniskās identifikācijas līdzekļu tehniskās un drošības specifikācijas.

Minētos īstenošanas aktus pieņem saskaņā ar pārbaudes procedūru, kas minēta 48. panta 2. punktā.

9. pants

Paziņošana

1. Paziņotāja dalībvalsts Komisijai paziņo turpmāk minēto informāciju un bez nepamatotas kavēšanās jebkādas turpmākas izmaiņas tajā:

a) elektroniskās identifikācijas shēmas aprakstu, tostarp attiecībā uz tās uzticamības līmeņiem un elektroniskās identifikācijas līdzekļu izsniedzēju vai izsniedzējiem saskaņā ar shēmu;

b) piemērojamo uzraudzības režīmu un informāciju par atbildības režīmu attiecībā uz:

i) pusi, kas izsniedz elektroniskās identifikācijas līdzekļus; un

ii) autentifikācijas procedūru veicošo pusi;

c) iestādi vai iestādēm, kas ir atbildīga(-as) par elektroniskās identifikācijas shēmu;

d) informāciju par vienību vai vienībām, kas pārvalda unikālo personas identifikācijas datu reģistrāciju;

e) aprakstu, kurā izklāstīts, kā tiek pildītas prasības, kas izklāstītas 12. panta 8. punktā minētajos īstenošanas aktos;

f) šīs regulas 7. panta f) punktā minētās autentifikācijas aprakstu;

g) paziņotās elektroniskās identifikācijas shēmas vai autentifikācijas, vai attiecīgo kompromitēto daļu apturēšanas vai atsaukšanas kārtību.

2. Vienu gadu pēc 8. panta 3. punktā un 12. panta 8. punktā minēto īstenošanas aktu piemērošanas dienas Komisija *Eiropas Savienības Oficiālajā Vēstnesī* publicē to elektroniskās identifikācijas shēmu sarakstu, par kurām iesniegts paziņojums saskaņā ar šā panta 1. punktu, un pamatinformāciju par attiecīgajām shēmām.

3. Ja Komisija paziņojumu saņem pēc tam, kad ir beidzies 2. punktā minētais termiņš, tā *Eiropas Savienības Oficiālajā Vēstnesī* publicē grozījumus 2. punktā minētajā sarakstā divos mēnešos pēc minētā paziņojuma saņemšanas dienas.

4. Dalībvalsts var iesniegt Komisijai prasību no 2. punktā minētā saraksta izņemt elektroniskās identifikācijas shēmu, par kuru minētā dalībvalsts ir iesniegusi paziņojumu. Komisija mēneša laikā pēc dalībvalsts pieprasījuma saņemšanas dienas *Eiropas Savienības Oficiālajā Vēstnesī* publicē atbilstošos grozījumus sarakstā.

5. Komisija ar īstenošanas aktiem var noteikt tos nosacījumus, formātus un procedūras, kas jāievēro saistībā ar paziņojumiem saskaņā ar 1. punktu. Minētos īstenošanas aktus pieņem saskaņā ar pārbaudes procedūru, kas minēta 48. panta 2. punktā.

10. pants

Drošības pasākumu pārkāpumi

1. Ja saistībā ar elektroniskās identifikācijas shēmu, kas paziņota saskaņā ar 9. panta 1. punktu, vai autentifikāciju, kas minēta 7. panta f) punktā, ir konstatēts pārkāpums vai ja tā ir daļēji kompromitēta tādā veidā, kas ietekmē minētās shēmas pārrobežu autentifikācijas uzticamību, paziņotāja dalībvalsts nekavējoties aptur vai atsauc minēto pārrobežu autentifikāciju vai attiecīgās apdraudētās daļas un informē citas dalībvalstis un Komisiju.

2. Ja 1. punktā minētais pārkāpums vai kompromitējums ir novērsts, paziņotāja dalībvalsts bez nepamatotas kavēšanās atjauno pārrobežu autentifikāciju un informē citas dalībvalstis un Komisiju.

3. Ja 1. punktā minētais pārkāpums vai kompromitējums netiek novērsts trīs mēnešos pēc apturēšanas vai atsaukšanas, paziņotāja dalībvalsts paziņo citām dalībvalstīm un Komisijai par elektroniskās identifikācijas shēmas anulēšanu.

Komisija bez nepamatotas kavēšanās publicē *Eiropas Savienības Oficiālajā Vēstnesī* 9. panta 2. punktā minētā saraksta attiecīgos grozījumus.

11. pants

Atbildība

1. Paziņotāja dalībvalsts ir atbildīga par zaudējumu, kas apzināti vai nolaidības dēļ radies jebkurai fiziskai vai juridiskai personai tādēļ, ka pārrobežu darījumā nav ievēroti pienākumi, kas tai ir noteikti 7. panta d) un f) punktā.

2. Elektroniskās identifikācijas līdzekļus izsniedzošā puse ir atbildīga par zaudējumu, kas apzināti vai nolaidības dēļ radies jebkurai fiziskai vai juridiskai personai tādēļ, ka pārrobežu darījumā nav ievērots 7. panta e) punktā minētais pienākums.

3. Autentifikācijas procedūru veicošā puse ir atbildīga par zaudējumu, kas apzināti vai nolaidības dēļ radies jebkurai fiziskai vai juridiskai personai tādēļ, ka pārrobežu darījumā nav nodrošināta 7. panta f) punktā minētās autentifikācijas pareiza veikšana.

4. Šā panta 1., 2. un 3. punktu piemēro saskaņā ar valstu noteikumiem par atbildību.

5. Saskaņā ar valsts tiesību aktiem 1., 2. un 3. punkts neskar to pušu atbildību, kuras veic darījumu, izmantojot tādā elektroniskās identifikācijas shēmā ietvertos elektroniskās identifikācijas līdzekļus, par kuru ir paziņots, ievērojot 9. panta 1. punktu.

12. pants

Sadarbība un sadarbspēja

1. Valsts elektroniskās identifikācijas shēmas, par kurām ir paziņots, ievērojot 9. panta 1. punktu, ir sadarbspējīgas.

2. Šā panta 1. punkta vajadzībām izveido sadarbspējas sistēmu.

3. Sadarbspējas sistēma atbilst šādiem kritērijiem:

a) tās mērķis ir būt tehnoloģiski neitrālai un tā nediskriminē nevienu konkrētu valsts tehnisko risinājumu attiecībā uz elektronisko identifikāciju dalībvalstī;

b) ja iespējams, tā atbilst Eiropas un starptautiskajiem standartiem;

c) tā sekmē integrētas privātuma aizsardzības principa īstenošanu; un

d) tā nodrošina personas datu apstrādi saskaņā ar Direktīvu 95/46/EK.

4. Sadarbspējas sistēma ietver:

a) atsauci uz minimālajām tehniskajām prasībām, kas ir saistītas ar 8. pantā minētajiem uzticamības līmeņiem;

b) paziņoto elektroniskās identifikācijas shēmu valsts uzticamības līmeņu attiecināšanu uz 8. pantā minētajiem uzticamības līmeņiem;

c) atsauci uz minimālajām tehniskajām prasībām attiecībā uz sadarbspēju;

d) atsauci uz personas identifikācijas datu minimālo kopumu, kas unikāli apliecina fizisko vai juridisko personu un kas ir pieejams elektroniskās identifikācijas shēmās;

e) procesuālo kārtību;

f) strīdu izšķiršanas kārtību; un

g) kopīgus operatīvās drošības standartus.

5. Dalībvalstis sadarbojas šādās jomās:

a) elektroniskās identifikācijas shēmu, par kurām iesniegti paziņojumi saskaņā ar 9. panta 1. punktu, un elektroniskās identifikācijas shēmu, par kurām dalībvalstis plāno paziņot, sadarbspēja; un

b) elektroniskās identifikācijas shēmu drošība.

6. Dalībvalstu sadarbība ietver:

a) informācijas, pieredzes un labas prakses apmaiņu attiecībā uz elektroniskās identifikācijas shēmām un jo īpaši tehniskajām prasībām, kas ir saistītas ar sadarbspēju un uzticamības līmeņiem;

b) informācijas, pieredzes un labas prakses apmaiņu attiecībā uz elektroniskās identifikācijas shēmu uzticamības līmeņiem saskaņā ar 8. pantu;

c) to elektroniskās identifikācijas shēmu salīdzinošo izvērtēšanu, uz kurām attiecas šī regula; un

d) attiecīgo attīstības tendenču izpēti elektroniskās identifikācijas nozarē.

7. Līdz 2015. gada 18. martam, pieņemot īstenošanas aktus, Komisija nosaka vajadzīgo procesuālo kārtību, lai veicinātu 5. un 6. punktā minēto dalībvalstu sadarbību, kas sekmētu riska pakāpei atbilstošu augsta līmeņa uzticamību un drošību.

8. Līdz 2015. gada 18. septembrim, lai noteiktu vienādus nosacījumus 1. punktā minētās prasības īstenošanai, Komisija, ievērojot 3. punktā izklāstītos kritērijus un ņemot vērā dalībvalstu sadarbības rezultātus, pieņem īstenošanas aktus attiecībā uz 4. punktā izklāstīto sadarbspējas sistēmu.

9. Šā panta 7. un 8. punktā minētos īstenošanas aktus pieņem saskaņā ar pārbaudes procedūru, kas minēta 48. panta 2. punktā.

III NODAĻA

UZTICAMĪBAS PAKALPOJUMI

1. IEDAĻA

Vispārīgi noteikumi

13. pants

Atbildība un pierādīšanas pienākums

1. Neskarot 2. punktu, uzticamības pakalpojumu sniedzēji ir atbildīgi par zaudējumu, kas apzināti vai nolaidības dēļ radīts jebkurai fiziskai vai juridiskai personai tādēļ, ka nav ievēroti šajā regulā minētie pienākumi.

Pienākumu pierādīt nekvalificēta uzticamības pakalpojumu sniedzēja nodomu vai nolaidību uzņemas fiziska vai juridiska persona, kas iesniedz prasību par šā punkta pirmajā daļā minēto zaudējumu.

Tiek uzskatīts, ka ir bijis nodoms vai nolaidība no kvalificēta uzticamības pakalpojumu sniedzēja puses, ja vien minētais kvalificēts uzticamības pakalpojumu sniedzējs nepierāda, ka šā punkta pirmajā daļā minētais zaudējums ir noticis bez nodoma vai nolaidības no minētā kvalificēta uzticamības pakalpojumu sniedzēja puses.

2. Ja uzticamības pakalpojumu sniedzējs iepriekš laikus informē savus klientus par tā sniegto pakalpojumu lietošanas ierobežojumiem un ja minētie ierobežojumi ir trešām personām atpazīstami, uzticamības pakalpojumu sniedzējs nav atbildīgs par zaudējumiem, kas rodas izmantojot pakalpojumus, kuri pārsniedz norādītos ierobežojumus.

3. Šā panta 1. un 2. punktu piemēro saskaņā ar valstu noteikumiem par atbildību.

14. pants

Starptautiskie aspekti

1. Ja trešās valsts izcelsmes uzticamības pakalpojumi ir atzīti saskaņā ar nolīgumu, kas saskaņā ar LESD 218. pantu noslēgts starp Savienību un attiecīgo trešo valsti vai starptautisku organizāciju, tad uzticamības pakalpojumus, ko sniedz uzticamības pakalpojumu sniedzēji, kas veic uzņēmējdarbību trešās valstīs, atzīst kā juridiski līdzvērtīgus kvalificētiem uzticamības pakalpojumiem, ko sniedz kvalificēti uzticamības pakalpojumu sniedzēji, kas veic uzņēmējdarbību Savienībā.

2. Ar 1. punktā minētajiem nolīgumiem nodrošina jo īpaši, ka:

a) prasības, kuras piemērojamas kvalificētiem uzticamības pakalpojumu sniedzējiem, kas veic uzņēmējdarbību Savienībā, un to sniegtajiem kvalificētiem uzticamības pakalpojumiem, ievēro uzticamības pakalpojumu sniedzēji trešā valstī vai starptautiskās organizācijās, ar kurām ir noslēgts nolīgums, un ka šīs prasības ievēro arī attiecībā uz to sniegtajiem uzticamības pakalpojumiem;

b) kvalificētos uzticamības pakalpojumus, ko sniedz kvalificēti uzticamības pakalpojumu sniedzēji, kas veic uzņēmējdarbību Savienībā, atzīst kā juridiski līdzvērtīgus uzticamības pakalpojumiem, ko sniedz uzticamības pakalpojumu sniedzēji trešā valstī vai starptautiskā organizācija, ar ko ir noslēgts nolīgums.

15. pants

Pieejamība personām ar invaliditāti

Ja tas praktiski iespējams, piedāvātie uzticamības pakalpojumi un minēto pakalpojumu sniegšanā izmantotie tiešā lietotāja produkti ir pieejami personām ar invaliditāti.

16. pants

Sankcijas

Dalībvalstis paredz noteikumus par sankcijām, kas piemērojamas šīs regulas pārkāpumu gadījumā. Paredzētās sankcijas ir iedarbīgas, samērīgas un atturošas.

2. IEDAĻA

Uzraudzība

17. pants

Uzraudzības iestāde

1. Dalībvalstis izraugās uzraudzības iestādi, kas veic uzņēmējdarbību tās teritorijā, vai, pēc savstarpējas vienošanās ar citu dalībvalsti, uzraudzības iestādi, kas veic uzņēmējdarbību minētajā citā dalībvalstī. Minētā iestāde ir atbildīga par uzraudzības uzdevumiem dalībvalstī, kas veic izraudzīšanu.

Uzraudzības iestādēm piešķir pilnvaras un pienācīgus resursus, kas tām nepieciešami to uzdevumu izpildē.

2. Dalībvalstis paziņo Komisijai to attiecīgo uzraudzības iestāžu nosaukumus un adreses, ko tās ir izraudzījušās.

3. Uzraudzības iestādes uzdevumi ir šādi:

a) uzraudzīt kvalificētus uzticamības pakalpojumu sniedzējus, kuri veic uzņēmējdarbību izraudzīšanas dalībvalsts teritorijā, lai, veicot *ex ante* un *ex post* uzraudzības darbības, nodrošinātu, ka minētie kvalificētie uzticamības pakalpojumu sniedzēji un to sniegtie kvalificētie uzticamības pakalpojumi atbilst šajā regulā noteiktajām prasībām;

b) vajadzības gadījumā rīkoties attiecībā uz nekvalificētiem uzticamības pakalpojumu sniedzējiem, kuri veic uzņēmējdarbību izraudzīšanas dalībvalsts teritorijā, izmantojot *ex post* uzraudzības darbības, kad tiek saņemta informācija, ka minētie nekvalificētie uzticamības pakalpojumu sniedzēji vai to sniegtie uzticamības pakalpojumi, iespējams, neatbilst šajā regulā noteiktajām prasībām.

4. Piemērojot 3. punktu un ievērojot tajā noteiktos ierobežojumus, uzraudzības iestādes uzdevumi ietver jo īpaši:

a) sadarbību ar citām uzraudzības iestādēm un palīdzības sniegšanu tām saskaņā ar 18. pantu;

b) 20. panta 1. punktā un 21. panta 1. punktā minēto atbilstības novērtēšanas ziņojumu analīzi;

c) citu uzraudzības iestāžu un sabiedrības informēšanu par drošības pārkāpumiem vai integritātes zudumu saskaņā ar 19. panta 2. punktu;

d) ziņojuma sniegšanu Komisijai par savām galvenajām darbībām saskaņā ar šā panta 6. punktu;

e) revīzijas veikšanu vai lūgumu atbilstības novērtēšanas struktūrai veikt kvalificēto uzticamības pakalpojumu sniedzēju atbilstības novērtēšanu saskaņā ar 20. panta 2. punktu;

f) sadarbību ar datu aizsardzības iestādēm, jo īpaši bez nepamatotas kavēšanās tās informējot par kvalificēto uzticamības pakalpojumu sniedzēju revīzijas rezultātiem, ja šķiet, ka ir notikuši personas datu aizsardzības noteikumu pārkāpumi;

g) kvalifikācijas statusa piešķiršanu uzticamības pakalpojumu sniedzējiem un to sniegtajiem pakalpojumiem un šī statusa anulēšanu saskaņā ar 20. un 21. pantu;

h) tās struktūras informēšanu, kas ir atbildīga par 22. panta 3. punktā minēto valsts uzticamības sarakstu, par lēmumiem piešķirt vai anulēt kvalificētā statusu, ja vien minētā struktūra nav arī uzraudzības iestāde;

i) darbības pārtraukšanas plānu esamības un pareizas piemērošanas verifikāciju gadījumos, kad kvalificētais uzticamības pakalpojumu sniedzējs pārtrauc savas darbības, tostarp attiecībā uz to, kā tiek saglabāta informācijas pieejamība saskaņā ar 24. panta 2. punkta h) apakšpunktu;

j) prasību, lai uzticamības pakalpojumu sniedzēji labotu jebkuru šajā regulā noteikto prasību neizpildi.

5. Dalībvalstis var prasīt uzraudzības iestādei izveidot, uzturēt un atjaunināt uzticamības infrastruktūru saskaņā ar valstu tiesību aktos paredzētajiem nosacījumiem.

6. Katru gadu līdz 31. martam katra uzraudzības iestāde iesniedz Komisijai pārskatu par iepriekšējā kalendārā gada laikā veiktajām galvenajām darbībām kopā ar kopsavilkumu par pārkāpumiem, par kuriem uzticamības pakalpojumu sniedzēji paziņojuši saskaņā ar 19. panta 2. punktu.

7. Komisija dara 6. punktā minēto ikgadējo pārskatu pieejamu dalībvalstīm.

8. Komisija ar īstenošanas aktiem var noteikt tos formātus un procedūras, kas jāievēro saistībā ar 6. punktā minēto ziņojumu. Minētos īstenošanas aktus pieņem saskaņā ar pārbaudes procedūru, kas minēta 48. panta 2. punktā.

18. pants

Savstarpēja palīdzība

1. Uzraudzības iestādes sadarbojas, lai apmainītos ar labu praksi.

Uzraudzības iestāde pēc pamatota pieprasījuma no citas uzraudzības iestādes saņemšanas sniedz minētajai iestādei palīdzību, tādējādi panākot uzraudzības iestāžu darbību konsekventu īstenošanu. Savstarpējā palīdzība jo īpaši var ietvert informācijas pieprasījumus un uzraudzības pasākumus, piemēram, pieprasījumus veikt ar 20. un 21. pantā minētajiem atbilstības novērtēšanas ziņojumiem saistītas pārbaudes.

2. Uzraudzības iestāde, kurai ir lūgta palīdzība, var noraidīt minēto pieprasījumu, pamatojoties uz jebkuru no šādiem iemesliem:

a) uzraudzības iestāde nav kompetenta sniegt minēto palīdzību;

b) lūgtā palīdzība nav samērīga ar uzraudzības iestādes uzraudzības darbībām, kas veiktas saskaņā ar 17. pantu;

c) lūgtās palīdzības sniegšana būtu pretrunā šīs regulas noteikumiem.

3. Attiecīgā gadījumā dalībvalstis var pilnvarot to attiecīgās uzraudzības iestādes veikt kopīgu izmeklēšanu, kurā piedalās citu dalībvalstu uzraudzības iestāžu darbinieki. Attiecīgās dalībvalstis saskaņā ar valsts tiesību aktiem vienojas par kārtību un procedūrām attiecībā uz šādām kopīgām darbībām un izstrādā minēto kārtību un procedūras.

19. pants

Uzticamības pakalpojumu sniedzējiem piemērojamās drošības prasības

1. Kvalificēti un nekvalificēti uzticamības pakalpojumu sniedzēji veic piemērotus tehniskus un organizatoriskus pasākumus, lai pārvaldītu to sniegto uzticamības pakalpojumu drošībai radītos riskus. Ar minētajiem pasākumiem nodrošina drošības līmeni, kas ir samērīgs ar riska pakāpi, ņemot vērā jaunākos tehnoloģiskos sasniegumus. Jo īpaši veic pasākumus, lai novērstu un mazinātu drošības incidentu ietekmi un informētu ieinteresētās personas par jebkuru šādu incidentu negatīvo ietekmi.

2. Kvalificēti un nekvalificēti uzticamības pakalpojumu sniedzēji bez nepamatotas kavēšanās, bet jebkurā gadījumā 24 stundās pēc attiecīgās informācijas saņemšanas, paziņo uzraudzības iestādei un attiecīgā gadījumā citām attiecīgām struktūrām, piemēram, informācijas drošības jomā kompetentajai valsts struktūrai vai datu aizsardzības iestādei, par jebkuru tādu drošības pārkāpumu vai integritātes zudumu, kas būtiski ietekmē sniegtos uzticamības pakalpojumus vai tajos uzturētos personas datus.

Ja drošības pārkāpums vai integritātes zudums varētu nelabvēlīgi ietekmēt fizisku vai juridisku personu, kurai ir sniegts uzticamības pakalpojums, uzticamības pakalpojumu sniedzējs bez nepamatotas kavēšanās paziņo fiziskajai vai juridiskai personai par drošības pārkāpumu vai integritātes zudumu.

Vajadzības gadījumā, jo īpaši tad, ja drošības pārkāpums vai integritātes zudums skar divas vai vairākas dalībvalstis, informētā uzraudzības iestāde informē citu attiecīgo dalībvalstu uzraudzības iestādes un *ENISA*.

Ja informētā uzraudzības iestāde uzskata, ka drošības pārkāpuma vai integritātes zuduma publiskošana ir sabiedrības interesēs, tā informē sabiedrību vai pieprasa, lai to izdarītu uzticamības pakalpojumu sniedzējs.

3. Uzraudzības iestāde reizi gadā *ENISA* iesniedz kopsavilkumu par drošības pārkāpumiem un integritātes zudumu, par kuriem paziņojuši uzticamības pakalpojumu sniedzēji.

4. Komisija ar īstenošanas aktiem var:

a) sīkāk precizēt 1. punktā minētos pasākumus; un

b) noteikt formātus un procedūras, tostarp termiņus, kas jāievēro saistībā ar 2. punktu.

Minētos īstenošanas aktus pieņem saskaņā ar pārbaudes procedūru, kas minēta 48. panta 2. punktā.

3. IEDAĻA

Kvalificēti uzticamības pakalpojumi

20. pants

Kvalificētu uzticamības pakalpojumu sniedzēju uzraudzība

1. Kvalificētu uzticamības pakalpojumu sniedzēju revīziju par minēto pakalpojumu sniedzēju līdzekļiem vismaz ik pēc 24 mēnešiem veic atbilstības novērtēšanas struktūra. Revīzijas nolūks ir apstiprināt, ka kvalificētie uzticamības pakalpojumu sniedzēji un to sniegtie kvalificētie uzticamības pakalpojumi atbilst šajā regulā noteiktajām prasībām. Kvalificētie uzticamības pakalpojumu sniedzēji trīs darba dienās pēc iegūtā atbilstības novērtēšanas ziņojuma saņemšanas to iesniedz uzraudzības iestādei.

2. Neskarot 1. punktu, uzraudzības iestāde var jebkurā laikā veikt revīziju vai lūgt atbilstības novērtēšanas struktūrai veikt kvalificēto uzticamības pakalpojumu sniedzēju atbilstības novērtēšanu par minēto uzticamības pakalpojumu sniedzēju līdzekļiem, lai apstiprinātu, ka tie un to sniegtie kvalificētie uzticamības pakalpojumi atbilst šajā regulā noteiktajām prasībām. Ja personas datu aizsardzības noteikumi, iespējams, ir pārkāpti, uzraudzības iestāde par revīzijas rezultātiem informē datu aizsardzības iestādes.

3. Ja uzraudzības iestāde pieprasa kvalificētam uzticamības pakalpojumu sniedzējam labot jebkādu šajā regulā noteikto prasību neizpildi un ja minētais pakalpojumu sniedzējs attiecīgi nerīkojas termiņā, ko attiecīgā gadījumā noteikusi uzraudzības iestāde, uzraudzības iestāde, ņemot vērā jo īpaši attiecīgās neizpildes apjomu, ilgumu un sekas,var anulēt attiecīgā pakalpojumu sniedzēja vai konkrētā skartā sniegtā pakalpojuma kvalifikācijas statusu un informēt 22. panta 3. punktā minēto iestādi, lai tiktu atjaunināti 22. panta 1. punktā minētie uzticamības saraksti. Uzraudzības iestāde informē kvalificēto uzticamības pakalpojumu sniedzēju par tā kvalifikācijas statusa vai attiecīgā pakalpojuma kvalifikācijas statusa anulēšanu.

4. Komisija ar īstenošanas aktiem var ieviest identifikācijas numurus šādiem standartiem:

a) atbilstības novērtēšanas struktūru akreditācijai un 1. punktā minētajam atbilstības novērtēšanas ziņojumam;

b) to revīzijas noteikumiem, kurus ievērojot, atbilstības novērtēšanas struktūras, kā minēts 1. punktā, vērtēs kvalificēto uzticamības pakalpojumu sniedzēju atbilstību.

Minētos īstenošanas aktus pieņem saskaņā ar pārbaudes procedūru, kas minēta 48. panta 2. punktā.

21. pants

Kvalificētu uzticamības pakalpojumu sniegšanas uzsākšana

1. Ja uzticamības pakalpojumu sniedzēji, kuriem nav kvalificētā statusa, plāno sākt sniegt kvalificētos uzticamības pakalpojumus, tie uzraudzības iestādei iesniedz paziņojumu par savu nodomu kopā ar atbilstības novērtēšanas ziņojumu, ko izsniegusi atbilstības novērtēšanas struktūra.

2. Uzraudzības iestāde verificē, vai uzticamības pakalpojumu sniedzējs un tā sniegtie uzticamības pakalpojumi atbilst šajā regulā noteiktajām prasībām, un jo īpaši prasībām, kas noteiktas kvalificētiem uzticamības pakalpojumu sniedzējiem un to sniegtajiem kvalificētiem uzticamības pakalpojumiem.

Ja uzraudzības iestāde secina, ka uzticamības pakalpojumu sniedzējs un tā sniegtie uzticamības pakalpojumi atbilst pirmajā daļā minētajām prasībām, uzraudzības iestāde vēlākais trīs mēnešos pēc paziņojuma saņemšanas piešķir kvalificētā statusu uzticamības pakalpojumu sniedzējam un tā sniegtajiem uzticamības pakalpojumiem un informē 22. panta 3. punktā minēto struktūru, lai saskaņā ar šā panta 1. punktu atjauninātu 22. panta 1. punktā minētos uzticamības sarakstus.

Ja trīs mēnešos no paziņojuma saņemšanas verificēšana nav pabeigta, uzraudzības iestāde informē uzticamības pakalpojumu sniedzēju, norādot kavēšanās iemeslus un termiņu, līdz kuram verifikācija jāpabeidz.

3. Kvalificēts uzticamības pakalpojumu sniedzējs var sākt sniegt kvalificēto uzticamības pakalpojumu pēc tam, kad 22. panta 1. punktā minētajos uzticamības sarakstos ir norādīts kvalificētā statuss.

4. Komisija ar īstenošanas aktiem var noteikt formātus un procedūras, kas jāievēro saistībā ar 1. un 2. punktu. Minētos īstenošanas aktus pieņem saskaņā ar pārbaudes procedūru, kas minēta 48. panta 2. punktā.

22. pants

Uzticamības saraksti

1. Katra dalībvalsts izveido, uztur un publicē uzticamības sarakstus, tostarp informāciju par kvalificētajiem uzticamības pakalpojumu sniedzējiem, par kuriem tā ir atbildīga, kā arī informāciju par to sniegtajiem kvalificētajiem uzticamības pakalpojumiem.

2. Dalībvalstis drošā veidā izveido, uztur un publicē 1. punktā minētos uzticamības sarakstus, kuri ir elektroniski parakstīti vai apzīmogoti, turklāt sagatavoti automatizētai apstrādei piemērotā formātā.

3. Dalībvalstis bez nepamatotas kavēšanās paziņo Komisijai informāciju par struktūru, kura ir atbildīga par valsts uzticamības sarakstu izveidi, uzturēšanu un publicēšanu, un sīku informāciju par to, kur šādi saraksti ir publicēti, par sertifikātiem, kas izmantoti uzticamības sarakstu parakstīšanai vai apzīmogošanai, un par visām attiecīgajām izmaiņām.

4. Izmantojot drošu kanālu, Komisija publisko 3. punktā minēto informāciju, kura ir elektroniski parakstīta vai apzīmogota un sagatavota automatizētai apstrādei piemērotā formātā.

5. Līdz 2015. gada 18. septembrim Komisija ar īstenošanas aktiem precizē 1. punktā minēto informāciju un nosaka uzticamības sarakstu tehniskās specifikācijas un formātus, kas jāievēro saistībā ar 1. līdz 4. punktu. Minētos īstenošanas aktus pieņem saskaņā ar pārbaudes procedūru, kas minēta 48. panta 2. punktā.

23. pants

Kvalificētu uzticamības pakalpojumu ES marķējums

1. Pēc tam, kad 22. panta 1. punkta minētajos uzticamības sarakstos ir norādīts 21. panta 2. punkta otrajā daļā minētais kvalificētā statuss, kvalificēti uzticamības pakalpojumu sniedzēji var izmantot ES marķējumu, lai vienkāršā, atpazīstamā un skaidrā veidā norādītu to sniegtos kvalificētos uzticamības pakalpojumus.

2. Izmantojot ES marķējumu attiecībā uz 1. punktā minētajiem kvalificētajiem uzticamības pakalpojumiem, kvalificēti uzticamības pakalpojumu sniedzēji nodrošina, ka to tīmekļa vietnē ir pieejama saite uz attiecīgo uzticamības sarakstu.

3. Līdz 2015. gada 1. jūlijam Komisija ar īstenošanas aktiem sniedz precizējumus attiecībā uz kvalificētu uzticamības pakalpojumu ES marķējuma formu un jo īpaši tā izskatu, saturu, izmēriem un koncepciju. Minētos īstenošanas aktus pieņem saskaņā ar pārbaudes procedūru, kas minēta 48. panta 2. punktā.

24. pants

Prasības kvalificētiem uzticamības pakalpojumu sniedzējiem

1. Izsniedzot kvalificētu sertifikātu uzticamības pakalpojumam, ar piemērotiem līdzekļiem un saskaņā ar valsts tiesību aktiem kvalificēts uzticamības pakalpojumu sniedzējs verificē tās fiziskās vai juridiskās personas identitāti, kurai izsniegts kvalificēts sertifikāts, un, ja vajadzīgs, šīs personas īpašās raksturīgās pazīmes.

Kvalificētais uzticamības pakalpojumu sniedzējs tieši vai paļaujoties uz trešo personu saskaņā ar valsts tiesību aktiem pirmajā daļā minēto informāciju verificē:

a) fiziskās personas vai juridiskās personas pilnvarotā pārstāvja klātbūtnē; vai

b) attālināti, izmantojot elektroniskās identifikācijas līdzekļus, attiecībā uz kuriem pirms kvalificētā sertifikāta izsniegšanas tika nodrošināta fiziskās personas vai juridiskās personas pilnvarotā pārstāvja klātbūtne un kuri atbilst 8. pantā izklāstītajām prasībām attiecībā uz "būtisku" vai "augstu" uzticamības līmeni, vai

c) izmantojot kvalificētu elektronisko parakstu vai kvalificētu elektronisko zīmogu; kas izsniegti saskaņā ar a) vai b) apakšpunktu; vai

d) izmantojot citas identifikācijas metodes, kuras ir atzītas valsts līmenī un kuras nodrošina fiziskai klātbūtnei līdzvērtīgu uzticamību. Atbilstības novērtēšanas struktūra apstiprina līdzvērtīgu uzticamību.

2. Kvalificēts uzticamības pakalpojumu sniedzējs, nodrošinot kvalificētus uzticamības pakalpojumus:

a) informē uzraudzības iestādi par visām izmaiņām kvalificēto uzticamības pakalpojumu sniegšanā un par nodomu pārtraukt minētās darbības;

b) nodarbina darbiniekus un vajadzības gadījumā apakšuzņēmējus, kuriem ir vajadzīgās zināšanas, uzticamība, pieredze un kvalifikācija un kuri un ir saņēmuši atbilstīgu apmācību par drošības un personas datu aizsardzības noteikumiem un piemēro Eiropas vai starptautiskiem standartiem atbilstīgas administratīvās un vadības procedūras;

c) attiecībā uz risku sakarā ar atbildību par zaudējumiem saskaņā ar 13. pantu nodrošina pietiekamus finanšu resursus un/vai iegūst piemērotu atbildības apdrošināšanu atbilstīgi valsts tiesību aktiem;

d) pirms iesaistīšanās līgumsaistībās skaidri un visaptveroši informē jebkuru personu, kura vēlas izmantot kvalificētus uzticamības pakalpojumus, par noteikumiem attiecībā uz minētā pakalpojuma izmantošanu, tostarp jebkurus tā izmantošanas ierobežojumus;

e) izmanto uzticamas sistēmas un produktus, kas ir aizsargāti pret izmaiņām un nodrošina to piedāvāto procesu tehnisko drošību un uzticamību;

f) izmanto uzticamas sistēmas tiem iesniegto datu uzglabāšanai verificējamā formā, lai:

i) šie dati būtu publiski pieejami izguves nolūkā tikai tad, ja tam piekrīt persona, uz kuru attiecas izsniegtie dati;

ii) glabāto datu ierakstus un izmaiņas varētu izdarīt tikai pilnvarotas personas;

iii) varētu pārbaudīt datu autentiskumu;

g) veic piemērotus pasākumus pret datu viltošanu un zādzību;

h) uz attiecīgu laikposmu, tostarp pēc tam, kad kvalificētais uzticamības pakalpojumu sniedzējs ir izbeidzis darbību, reģistrē un nodrošina pieejamu visu attiecīgo informāciju par kvalificētā uzticamības pakalpojumu sniedzēja izsniegtajiem un saņemtajiem datiem, jo īpaši tādēļ, lai sniegtu pierādījumus tiesvedībā un lai nodrošinātu pakalpojuma nepārtrauktību. Šādu reģistrāciju var veikt elektroniski;

i) ir sagatavojuši aktuālu darbības pārtraukšanas plānu, lai garantētu pakalpojumu nepārtrauktību atbilstoši noteikumiem, ko saskaņā ar 17. panta 4. punkta i) apakšpunktu ir verificējusi uzraudzības iestāde;

j) garantē personas datu likumīgu apstrādi saskaņā ar Direktīvu 95/46/EK;

k) gadījumā, ja kvalificēti uzticamības pakalpojumu sniedzēji izsniedz kvalificētus sertifikātus, izveido un atjaunina sertifikātu datubāzi.

3. Ja kvalificēts uzticamības pakalpojumu sniedzējs, kas izsniedz kvalificētus sertifikātus, nolemj atsaukt sertifikātu, tas reģistrē šādu atsaukumu savā sertifikātu datubāzē un laicīgi – jebkurā gadījumā 24 stundās pēc lūguma saņemšanas – publicē sertifikāta atsaukšanas statusu. Atsaukums stājas spēkā uzreiz pēc tā publicēšanas.

4. Attiecībā uz 3. punktu kvalificēti uzticamības pakalpojumu sniedzēji, kas izsniedz kvalificētus sertifikātus, ikvienai atkarīgajai pusei sniedz informāciju par tiem izsniegto kvalificēto sertifikātu derīgumu vai atsaukšanu. Šī informācija ir pieejama vismaz par katru sertifikātu jebkurā laikā un pēc sertifikāta derīguma termiņa beigām, automatizētā veidā, kas ir uzticams, bez maksas un efektīvs.

5. Komisija ar īstenošanas aktiem var ieviest uzticamu sistēmu un produktu standartu identifikācijas numurus, kas atbilst šā panta 2. punkta e) un f) apakšpunktā noteiktajām prasībām. Uzskata, ka atbilstība šajā pantā noteiktajām prasībām ir panākta tad, ja uzticamas sistēmas un produkti atbilst minētajiem standartiem. Minētos īstenošanas aktus pieņem saskaņā ar pārbaudes procedūru, kas minēta 48. panta 2. punktā.

4. IEDAĻA

Elektroniskie paraksti

25. pants

Elektronisko parakstu juridiskais spēks

1. Elektroniskajam parakstam ir neapšaubāms juridiskais spēks, tas ir pieņemams kā pierādījums tiesvedībā, un to nedrīkst noraidīt tikai elektroniskā formāta dēļ vai tādēļ, ka tas neatbilst kvalificētu elektronisko parakstu prasībām.

2. Kvalificēts elektronisks paraksts juridiskā spēka ziņā ir līdzvērtīgs parakstam ar roku.

3. Kvalificētu elektronisko parakstu, kura pamatā ir vienā dalībvalstī izsniegts kvalificēts sertifikāts, atzīst kā kvalificētu elektronisko parakstu visās citās dalībvalstīs.

26. pants

Prasības uzlabotiem elektroniskajiem parakstiem

Uzlabots elektroniskais paraksts atbilst šādām prasībām:

a) tas ir unikālā veidā saistīts ar parakstītāju;

b) tas spēj identificēt parakstītāju;

c) tas radīts ar elektroniskā paraksta radīšanas datiem, kuru izmantošanu ar augstu ticamības līmeni var kontrolēt tikai un vienīgi parakstītājs; un

d) tas ir saistīts ar parakstītajiem datiem tādā veidā, lai būtu atklājamas jebkādas turpmākas to izmaiņas.

27. pants

Elektroniskie paraksti sabiedrisko pakalpojumu jomā

1. Ja dalībvalsts pieprasa uzlabotu elektronisko parakstu, lai lietotu publiskās iestādes piedāvātus vai tās vārdā veiktus tiešsaistes pakalpojumus, minētā dalībvalsts atzīst uzlabotus elektroniskos parakstus, uzlabotus elektroniskos parakstus, kuru pamatā ir kvalificēts elektronisko parakstu sertifikāts, un kvalificētus elektroniskos parakstus vismaz tādos formātos vai izmantojot tādas metodes, kas definētas 5. punktā minētajos īstenošanas aktos.

2. Ja dalībvalsts pieprasa uzlabotu elektronisko parakstu, kura pamatā ir kvalificēts sertifikāts, lai lietotu publiskās iestādes piedāvātus vai tās vārdā veiktus tiešsaistes pakalpojumus, minētā dalībvalsts atzīst uzlabotus elektroniskos parakstus, kuru pamatā ir kvalificēts sertifikāts, un kvalificētus elektroniskos parakstus vismaz tādos formātos vai izmantojot tādas metodes, kas definētas 5. punktā minētajos īstenošanas aktos.

3. Attiecībā uz publiskās iestādes piedāvātu tiešsaistes pakalpojumu pārrobežu lietošanu dalībvalstis nepieprasa elektronisku parakstu ar tādu drošības līmeni, kas ir augstāks nekā kvalificētajam elektroniskam parakstam.

4. Komisija ar īstenošanas aktiem var ieviest uzlabotu elektronisko parakstu standartu identifikācijas numurus. Ja uzlabots elektroniskais paraksts atbilst minētajiem standartiem, uzskata, ka uzlabots elektroniskais paraksts atbilst šā panta 1. un 2. punktā un 26. pantā minētajām prasībām. Minētos īstenošanas aktus pieņem saskaņā ar pārbaudes procedūru, kas minēta 48. panta 2. punktā.

5. Līdz 2015. gada 18. septembrim un ņemot vērā pastāvošo praksi, standartus un Savienības tiesību aktus, Komisija ar īstenošanas aktiem nosaka uzlabotu elektronisko parakstu atsauces formātus vai atsauces metodes gadījumiem, kad tiek izmantoti alternatīvi formāti. Minētos īstenošanas aktus pieņem saskaņā ar pārbaudes procedūru, kas minēta 48. panta 2. punktā.

28. pants

Kvalificēti elektronisko parakstu sertifikāti

1. Kvalificēti elektronisko parakstu sertifikāti atbilst I pielikumā noteiktajām prasībām.

2. Uz kvalificētiem elektronisko parakstu sertifikātiem neattiecas neviena obligātā prasība, kas pārsniedz I pielikumā noteiktās prasības.

3. Kvalificēti elektronisko parakstu sertifikāti var ietvert papildu raksturīgas pazīmes, kas nav obligātas. Minētās pazīmes neskar kvalificētu elektronisko parakstu sadarbspēju un atzīšanu.

4. Ja kvalificēts elektronisko parakstu sertifikāts ir atsaukts pēc sākotnējas aktivizēšanas, tas vairs nav derīgs no tā atsaukšanas brīža, un tā statusu nekādā gadījumā nevar mainīt.

5. Dalībvalstis var noteikt valsts noteikumus par kvalificēta elektroniskā paraksta sertifikāta pagaidu apturēšanu, ievērojot šādus nosacījumus:

a) ja kvalificētam elektroniskā paraksta sertifikātam piemēro pagaidu apturēšanu, minētais sertifikāts zaudē derīgumu uz apturēšanas laikposmu;

b) apturēšanas laikposmu skaidri norāda sertifikātu datubāzē, un apturēšanas statuss apturēšanas laikposmā ir redzams pakalpojuma sniegšanas informācijā par sertifikāta statusu.

6. Komisija ar īstenošanas aktiem var ieviest kvalificētu elektroniskā paraksta sertifikātu standartu identifikācijas numurus. Uzskata, ka atbilstība I pielikumā noteiktajām prasībām ir panākta tad, ja kvalificēts elektroniskā paraksta sertifikāts atbilst minētajiem standartiem. Minētos īstenošanas aktus pieņem saskaņā ar pārbaudes procedūru, kas minēta 48. panta 2. punktā.

29. pants

Prasības kvalificētām elektroniskā paraksta radīšanas ierīcēm

1. Kvalificētas elektroniskā paraksta radīšanas ierīces atbilst II pielikumā noteiktajām prasībām.

2. Komisija ar īstenošanas aktiem var ieviest kvalificētu elektroniskā paraksta radīšanas ierīču standartu identifikācijas numurus. Uzskata, ka atbilstība II pielikumā noteiktajām prasībām ir panākta tad, ja kvalificētas elektroniskā paraksta radīšanas ierīces atbilst minētajiem standartiem. Minētos īstenošanas aktus pieņem saskaņā ar pārbaudes procedūru, kas minēta 48. panta 2. punktā.

30. pants

Kvalificētu elektroniskā paraksta radīšanas ierīču sertifikācija

1. Kvalificētu elektroniskā paraksta radīšanas ierīču atbilstību II pielikumā noteiktajām prasībām sertificē dalībvalstu izraudzītas attiecīgas publiskās vai privātās iestādes.

2. Dalībvalstis paziņo Komisijai 1. punktā minēto valsts vai privātā sektora iestāžu nosaukumus un adreses. Komisija minēto informāciju dara pieejamu dalībvalstīm.

3. Šā panta 1. punktā minētās sertifikācijas pamatā ir viena no šādām procedūrām:

a) drošības novērtēšanas procedūra, kas veikta saskaņā ar kādu no standartiem, kuri noteikti attiecībā uz tādu informācijas tehnoloģiju produktu drošības novērtēšanu, kuri iekļauti sarakstā, kas izveidots saskaņā ar otro daļu; vai

b) cita procedūra, kas nav minēta a) apakšpunktā, ar noteikumu, ka tā izmanto salīdzināmus drošības līmeņus un 1. punktā minētā publiskā vai privātā iestāde par minēto procedūru paziņo Komisijai. Minēto procedūru var izmantot tikai tad, ja nav a) apakšpunktā minēto standartu vai ja norit a) apakšpunktā minētā drošības novērtēšanas procedūra.

Komisija ar īstenošanas aktiem izveido tādu standartu sarakstu, kuri attiecas uz a) apakšpunktā minēto informācijas tehnoloģiju produktu drošības novērtēšanu. Minētos īstenošanas aktus pieņem saskaņā ar pārbaudes procedūru, kas minēta 48. panta 2. punktā.

4. Komisija tiek pilnvarota pieņemt deleģētos aktus saskaņā ar 47. pantu attiecībā uz tādu īpašu kritēriju izstrādi, kuri jāievēro šā panta 1. punktā minētajām izraudzītajām iestādēm.

31. pants

Sertificēto kvalificētu elektroniskā paraksta radīšanas ierīču saraksta publicēšana

1. Dalībvalstis bez nepamatotas kavēšanās un ne vēlāk kā vienu mēnesi pēc sertifikācijas pabeigšanas paziņo Komisijai informāciju par kvalificētām elektroniskā paraksta radīšanas ierīcēm, ko sertificējušas 30. panta 1. punktā minētās iestādes. Dalībvalstis bez nepamatotas kavēšanās un ne vēlāk kā vienu mēnesi pēc sertifikācijas anulēšanas Komisijai paziņo arī informāciju par tām elektroniskā paraksta radīšanas ierīcēm, kas vairs nav sertificētas.

2. Pamatojoties uz saņemto informāciju, Komisija izveido, publicē un atjaunina sarakstu, kurā uzskaitītas sertificētās kvalificētās elektroniskā paraksta radīšanas ierīces.

3. Komisija ar īstenošanas aktiem var noteikt tos formātus un procedūras, kas jāievēro saistībā ar 1. punktu. Minētos īstenošanas aktus pieņem saskaņā ar pārbaudes procedūru, kas minēta 48. panta 2. punktā.

32. pants

Prasības kvalificētu elektronisko parakstu validācijai

1. Kvalificēta elektroniskā paraksta validācijas procesā apstiprina kvalificēta elektroniskā paraksta derīgumu ar noteikumu, ka:

a) sertifikāts, kas apliecina parakstu, parakstīšanas brīdī bija kvalificēts elektroniskā paraksta sertifikāts atbilstīgi I pielikumam;

b) kvalificēto sertifikātu izsniedza kvalificēts uzticamības pakalpojumu sniedzējs, un tas parakstīšanas brīdī bija derīgs;

c) paraksta validācijas dati atbilst datiem, kurus sniedz atkarīgajai pusei;

d) unikālu datu kopums, kas apliecina sertifikātā minētā parakstītāja identitāti, ir pareizi nosūtīts atkarīgajai pusei;

e) ja parakstīšanas brīdī tika izmantots pseidonīms, tas ir skaidri norādīts atkarīgajai pusei;

f) elektroniskais paraksts tika izveidots ar kvalificētu elektroniskā paraksta radīšanas ierīci;

g) parakstīto datu integritāte nav kompromitēta;

h) parakstīšanas brīdī tika izpildītas 26. pantā noteiktās prasības;

2. Ar kvalificēta elektroniskā paraksta validēšanai izmantoto sistēmu atkarīgajai pusei tiek sniegti precīzi validēšanas rezultāti, ļaujot atkarīgajai pusei atklāt jebkādas ar drošību saistītas problēmas.

3. Komisija ar īstenošanas aktiem var ieviest kvalificētu elektronisko parakstu validācijas standartu identifikācijas numurus. Uzskata, ka atbilstība 1. punktā noteiktajām prasībām ir panākta tad, ja kvalificētu elektronisko parakstu validācija atbilst minētajiem standartiem. Minētos īstenošanas aktus pieņem saskaņā ar pārbaudes procedūru, kas minēta 48. panta 2. punktā.

33. pants

Kvalificētu elektronisko parakstu kvalificēti validēšanas pakalpojumi

1. Kvalificētu elektronisko parakstu kvalificētus validēšanas pakalpojumus var sniegt tikai kvalificēts uzticamības pakalpojumu sniedzējs, kurš:

a) veic validāciju atbilstīgi 32. panta 1. punktam; un

b) ļauj atkarīgajām pusēm saņemt validēšanas rezultātus automatizētā veidā, kas ir uzticams un efektīvs, nodrošinot, ka uz šā dokumenta ir kvalificēto validēšanas pakalpojumu sniedzēja uzlabots elektroniskais paraksts vai uzlabots elektroniskais zīmogs.

2. Komisija ar īstenošanas aktiem var ieviest 1. punktā minēto kvalificētu validēšanas pakalpojumu standartu identifikācijas numurus. Uzskata, ka atbilstība 1. punktā noteiktajām prasībām ir panākta tad, ja kvalificētu elektronisko parakstu validācija atbilst minētajiem standartiem. Minētos īstenošanas aktus pieņem saskaņā ar pārbaudes procedūru, kas minēta 48. panta 2. punktā.

34. pants

Kvalificētu elektronisko parakstu kvalificēti saglabāšanas pakalpojumi

1. Kvalificētu elektronisko parakstu kvalificētas saglabāšanas pakalpojumus var sniegt tikai kvalificēts uzticamības pakalpojumu sniedzējs, kas izmanto tādas procedūras un tehnoloģijas, ar kurām var nodrošināt kvalificētā elektroniskā paraksta uzticamību ilgāk par to tehnoloģiskā derīguma termiņu.

2. Komisija ar īstenošanas aktiem var ieviest kvalificētu elektronisko parakstu kvalificētas saglabāšanas pakalpojumu standartu identifikācijas numurus. Uzskata, ka atbilstība 1. punktā noteiktajām prasībām ir panākta tad, ja kvalificētu elektronisko parakstu kvalificētas saglabāšanas pakalpojumi atbilst minētajiem standartiem. Minētos īstenošanas aktus pieņem saskaņā ar pārbaudes procedūru, kas minēta 48. panta 2. punktā.

5. IEDAĻA

Elektroniskie zīmogi

35. pants

Elektronisko zīmogu juridiskais spēks

1. Elektroniskajam zīmogam ir neapšaubāms juridiskais spēks, tas ir pieņemams kā pierādījums tiesvedībā, un to nevar noraidīt tikai elektroniskā formāta dēļ vai tādēļ, ka tas neatbilst kvalificētu elektronisko zīmogu prasībām.

2. Attiecībā uz kvalificētu elektronisko zīmogu pastāv prezumpcija par minēto datu integritāti un to datu izcelsmes pareizību, ar kuriem kvalificētais elektronisko zīmogs ir saistīts.

3. Kvalificētu elektronisko zīmogu, kura pamatā ir vienā dalībvalstī izsniegts kvalificēts sertifikāts, atzīst kā kvalificētu elektronisko zīmogu visās citās dalībvalstīs.

36. pants

Prasības uzlabotiem elektroniskajiem zīmogiem

Uzlabots elektroniskais zīmogs atbilst šādām prasībām:

a) tas ir unikālā veidā saistīts ar zīmoga radītāju;

b) tas spēj identificēt zīmoga radītāju;

c) tas radīts ar elektroniskā zīmoga radīšanas datiem, kuru izmantošanu ar augstu ticamības līmeni var kontrolēt tikai un vienīgi zīmoga radītājs elektroniskā zīmoga radīšanai; un

d) tas ir saistīts ar attiecīgajiem datiem tādā veidā, lai būtu atklājamas jebkādas turpmākas to izmaiņas.

37. pants

Elektroniskie zīmogi sabiedrisko pakalpojumu jomā

1. Ja kāda dalībvalsts pieprasa uzlabotu elektronisko zīmogu, lai varētu lietot kādas publiskās iestādes piedāvātus vai tās vārdā veiktus tiešsaistes pakalpojumus, tad šī dalībvalsts atzīst uzlabotus elektroniskos zīmogus, uzlabotus elektroniskos zīmogus, kuru pamatā ir kvalificēts elektronisko zīmogu sertifikāts, un kvalificētus elektroniskos zīmogus vismaz tādos formātos vai izmantojot tādas metodes, kas definētas 5. punktā minētajos īstenošanas aktos.

2. Ja kāda dalībvalsts pieprasa uzlabotu elektronisko zīmogu, kura pamatā ir kvalificēts sertifikāts, lai varētu lietot kādas publiskās iestādes piedāvātus vai tās vārdā veiktus tiešsaistes pakalpojumus, tad šī dalībvalsts atzīst uzlabotus elektroniskos zīmogus, kuru pamatā ir kvalificēts sertifikāts, un kvalificētu elektronisko zīmogu vismaz tādos formātos vai izmantojot tādas metodes, kas definētas 5. punktā minētajos īstenošanas aktos.

3. Saistībā ar publiskās iestādes piedāvātu tiešsaistes pakalpojumu pārrobežu izmantojumu dalībvalstis nepieprasa elektronisku zīmogu ar tādu drošības nodrošinājuma līmeni, kas ir augstāks nekā kvalificētajam elektroniskam zīmogam.

4. Komisija ar īstenošanas aktiem var ieviest uzlabotu elektronisko zīmogu standartu identifikācijas numurus. Ja uzlabots elektroniskais zīmogs atbilst minētajiem standartiem, uzskata, ka uzlabots elektroniskais zīmogs atbilst šā panta 1. un 2. punktā un 36. pantā minētajām prasībām. Minētos īstenošanas aktus pieņem saskaņā ar pārbaudes procedūru, kas minēta 48. panta 2. punktā.

5. Līdz 2015. gada 18. septembrim un ņemot vērā pastāvošo praksi, standartus un Savienības tiesību aktus, Komisija ar īstenošanas aktiem nosaka uzlabotu elektronisko zīmogu atsauces formātus vai atsauces metodes gadījumiem, kad tiek izmantoti alternatīvi formāti. Minētos īstenošanas aktus pieņem saskaņā ar pārbaudes procedūru, kas minēta 48. panta 2. punktā.

38. pants

Kvalificēti elektronisko zīmogu sertifikāti

1. Kvalificēti elektronisko zīmogu sertifikāti atbilst III pielikumā noteiktajām prasībām.

2. Uz kvalificētiem elektronisko zīmogu sertifikātiem neattiecas neviena obligātā prasība, kas pārsniedz III pielikumā noteiktās prasības.

3. Kvalificēti elektronisko zīmogu sertifikāti var ietvert papildu raksturīgas pazīmes, kas nav obligātas. Minētās pazīmes neskar kvalificētu elektronisko zīmogu sadarbspēju un atzīšanu.

4. Ja kvalificēts elektroniskā zīmoga sertifikāts ir atsaukts pēc sākotnējas aktivizēšanas, tas vairs nav derīgs no tā atsaukšanas brīža, un tā statusu nekādā gadījumā nevar mainīt.

5. Dalībvalstis var paredzēt valsts noteikumus par kvalificētu elektronisko zīmogu sertifikātu pagaidu apturēšanu, ievērojot šādus nosacījumus:

a) ja kvalificētam elektroniskā zīmoga sertifikātam piemēro pagaidu apturēšanu, minētais sertifikāts zaudē derīgumu uz apturēšanas laikposmu;

b) apturēšanas laikposmu skaidri norāda sertifikātu datubāzē, un apturēšanas statuss apturēšanas laikposmā ir redzams pakalpojuma sniegšanas informācijā par sertifikāta statusu.

6. Komisija ar īstenošanas aktiem var ieviest kvalificētu elektronisko zīmogu sertifikātu standartu identifikācijas numurus. Uzskata, ka atbilstība III pielikumā noteiktajām prasībām ir panākta tad, ja kvalificēts elektroniskā zīmoga sertifikāts atbilst minētajiem standartiem. Minētos īstenošanas aktus pieņem saskaņā ar pārbaudes procedūru, kas minēta 48. panta 2. punktā.

39. pants

Kvalificētas elektroniskā zīmoga radīšanas ierīces

1. Prasībām, kas noteiktas attiecībā uz kvalificētām elektroniskā zīmoga radīšanas ierīcēm, 29. pantu piemēro *mutatis mutandis*.

2. Attiecībā uz kvalificēto elektroniskā zīmoga radīšanas ierīču sertifikāciju 30. pantu piemēro *mutatis mutandis*.

3. Attiecībā uz tāda saraksta publicēšanu, kurā uzskaitītas kvalificētas elektroniskā zīmoga radīšanas ierīces, kas ir sertificētas, 31. pantu piemēro *mutatis mutandis*.

40. pants

Kvalificētu elektronisko zīmogu validācija un saglabāšana

Attiecībā uz kvalificētu elektronisko zīmogu validāciju un saglabāšanu 32., 33. un 34. pantu piemēro *mutatis mutandis*.

6. IEDAĻA

Elektroniskie laika zīmogi

41. pants

Elektronisko laika zīmogu juridiskais spēks

1. Elektroniskajam laika zīmogam ir neapšaubāms juridiskais spēks, tas ir pieņemams kā pierādījums tiesvedībā, un to nevar noraidīt tikai elektroniskā formāta dēļ vai tādēļ, ka tas neatbilst kvalificētā elektroniskā laika zīmoga prasībām.

2. Attiecībā uz kvalificētu elektronisko laika zīmogu pastāv prezumpcija par tajā norādītā datuma un laika precizitāti un to datu integritāti, ar kuriem ir saistīts minētais datums un laiks.

3. Kvalificētu elektronisko laika zīmogu, kas izsniegts vienā dalībvalstī, atzīst kā kvalificētu elektronisko laika zīmogu visās dalībvalstīs.

42. pants

Prasības kvalificētiem elektroniskajiem laika zīmogiem

1. Kvalificēts elektroniskais laika zīmogs atbilst šādām prasībām:

a) tas saista datumu un laiku ar datiem tādā veidā, lai samērīgi nepieļautu iespēju veikt datos neatklājamas izmaiņas;

b) tas ir balstīts uz precīzu laika avotu, kas ir sasaistīts ar universālo koordinēto laiku; un

c) tas ir parakstīts, izmantojot kvalificētā uzticamības pakalpojumu sniedzēja uzlabotu elektronisko parakstu, vai apzīmogots ar uzlabotu elektronisko zīmogu vai izmantojot kādu līdzvērtīgu metodi.

2. Komisija ar īstenošanas aktiem var ieviest standartu identifikācijas numurus attiecībā uz datuma un laika sasaisti ar datiem un attiecībā uz precīziem laika avotiem. Uzskata, ka atbilstība 1. punktā noteiktajām prasībām ir panākta tad, ja datuma un laika sasaiste ar datiem un precīzais laika avots atbilst šiem standartiem. Minētos īstenošanas aktus pieņem saskaņā ar pārbaudes procedūru, kas minēta 48. panta 2. punktā.

7. IEDAĻA

Elektroniski reģistrēti piegādes pakalpojumi

43. pants

Elektroniski reģistrēta piegādes pakalpojuma juridiskais spēks

1. Datiem, kas nosūtīti un saņemti, izmantojot elektroniski reģistrētu piegādes pakalpojumu, ir juridiskais spēks un tie ir pieņemami kā pierādījums tiesvedībā, un tos nevar noraidīt tikai elektroniskā formāta dēļ vai tādēļ, ka tie neatbilst kvalificētā elektroniski reģistrētā piegādes pakalpojuma prasībām.

2. Attiecībā uz datiem, kas nosūtīti un saņemti, izmantojot kvalificētu elektroniski reģistrētu piegādes pakalpojumu, pastāv prezumpcija par datu integritāti, par to, ka minētos datus nosūtījis identificētais sūtītājs, ka tos saņēmis identificētais adresāts, un par kvalificētā elektroniski reģistrētā piegādes pakalpojumā norādīto datu nosūtīšanas un saņemšanas datuma un laika precizitāti.

44. pants

Prasības kvalificētiem elektroniski reģistrētiem piegādes pakalpojumiem

1. Kvalificēti elektroniski reģistrēti piegādes pakalpojumi atbilst šādām prasībām:

a) tos sniedz viens vai vairāki kvalificēti uzticamības pakalpojumu sniedzēji;

b) tie nodrošina augstu uzticamības pakāpi attiecībā uz sūtītāja identifikāciju;

c) pirms datu piegādes tie nodrošina adresāta identifikāciju;

d) datu nosūtīšanas un saņemšanas drošību apliecina ar kvalificēta uzticamības pakalpojumu sniedzēja uzlabotu elektronisko parakstu vai uzlabotu elektronisko zīmogu tādā veidā, lai nepieļautu iespēju veikt datos neatklājamas izmaiņas;

e) visas izmaiņas datos, kuras jāveic datu saņemšanas vai nosūtīšanas nolūkā, skaidri norāda datu nosūtītājam un adresātam;

f) datu nosūtīšanas, saņemšanas un jebkādu izmaiņu datumu un laiku norāda ar kvalificētu elektronisko laika zīmogu.

Ja datus pārsūta divu vai vairāku kvalificētu uzticamības pakalpojumu sniedzēju starpā, tad visiem kvalificētajiem uzticamības pakalpojumu sniedzējiem piemēro a) līdz f) apakšpunktā minētās prasības.

2. Komisija ar īstenošanas aktiem var ieviest datu nosūtīšanas un saņemšanas standartu identifikācijas numurus. Uzskata, ka atbilstība 1. punktā noteiktajām prasībām ir panākta tad, ja datu nosūtīšana un saņemšana atbilst minētajiem standartiem. Minētos īstenošanas aktus pieņem saskaņā ar pārbaudes procedūru, kas minēta 48. panta 2. punktā.

8. IEDAĻA

Tīmekļa vietņu autentifikācija

45. pants

Prasības kvalificētiem tīmekļa vietņu autentifikācijas sertifikātiem

1. Kvalificēti tīmekļa vietņu autentifikācijas sertifikāti atbilst IV pielikumā noteiktajām prasībām.

2. Komisija ar īstenošanas aktiem var ieviest kvalificētu tīmekļa vietņu autentifikācijas sertifikātu standartu identifikācijas numurus. Uzskata, ka atbilstība IV pielikumā noteiktajām prasībām ir panākta tad, ja kvalificēts tīmekļa vietņu autentifikācijas sertifikāts atbilst minētajiem standartiem. Minētos īstenošanas aktus pieņem saskaņā ar pārbaudes procedūru, kas minēta 48. panta 2. punktā.

IV NODAĻA

ELEKTRONISKIE DOKUMENTI

46. pants

Elektronisko dokumentu juridiskais spēks

Elektroniskajam dokumentam ir juridiskais spēks, tas ir pieņemams kā pierādījums tiesvedībā, un to nedrīkst noraidīt tikai elektroniskā formāta dēļ.

V NODAĻA

PILNVARU DELEĢĒŠANA UN ĪSTENOŠANAS NOTEIKUMI

47. pants

Deleģēšanas īstenošana

1. Pilnvaras pieņemt deleģētos aktus Komisijai piešķir, ievērojot šajā pantā izklāstītos nosacījumus.

2. Pilnvaras pieņemt 30. panta 4. punktā minētos deleģētos aktus Komisijai piešķir uz nenoteiktu laiku no 2014. gada 17. septembra.

3. Eiropas Parlaments vai Padome jebkurā laikā var atsaukt 30. panta 4. punktā minēto pilnvaru deleģēšanu. Ar lēmumu par atsaukšanu izbeidz tajā norādīto pilnvaru deleģēšanu. Lēmums stājas spēkā nākamajā dienā pēc tā publicēšanas *Eiropas Savienības Oficiālajā Vēstnesī* vai vēlākā dienā, kas tajā norādīta. Tas neskar jau spēkā esošos deleģētos aktus.

4. Tiklīdz tā pieņem deleģētu aktu, Komisija par to paziņo vienlaikus Eiropas Parlamentam un Padomei.

5. Saskaņā ar 30. panta 4. punktu pieņemts deleģētais akts stājas spēkā tikai tad, ja divos mēnešos no dienas, kad minētais akts paziņots Eiropas Parlamentam un Padomei, ne Eiropas Parlaments, ne Padome nav izteikuši iebildumus vai ja pirms minētā laikposma beigām gan Eiropas Parlaments, gan Padome ir informējuši Komisiju par savu nodomu neizteikt iebildumus. Pēc Eiropas Parlamenta vai Padomes iniciatīvas šo laikposmu pagarina par diviem mēnešiem.

48. pants

Komiteju procedūra

1. Komisijai palīdz komiteja. Minētā komiteja ir komiteja Regulas (ES) Nr. 182/2011 nozīmē.

2. Ja ir atsauce uz šo punktu, piemēro Regulas (ES) Nr. 182/2011 5. pantu.

VI NODAĻA

NOBEIGUMA NOTEIKUMI

49. pants

Pārskatīšana

Komisija pārskata šīs regulas piemērošanu un ziņo Eiropas Parlamentam un Padomei ne vēlāk kā 2020. gada 1. jūlijā. Komisija jo īpaši novērtē, vai ir lietderīgi grozīt šīs regulas darbības jomu vai konkrētus tās noteikumus, tostarp 6. pantu, 7. panta f) punktu un 34., 43., 44. un 45. pantu, ņemot vērā šīs regulas piemērošanā gūto pieredzi, kā arī tehnoloģiskos sasniegumus un attīstību tirgus un tiesiskajā jomā.

Attiecīgā gadījumā pirmajā daļā minētajam ziņojumam pievieno tiesību aktu priekšlikumus.

Turklāt Komisija iesniedz ziņojumu Eiropas Parlamentam un Padomei reizi četros gados pēc pirmajā daļā minētā ziņojuma par panākumiem šīs regulas mērķu īstenošanā.

50. pants

Atcelšana

1. Direktīvu 1999/93/EK atceļ no 2016. gada 1. jūlija.

2. Atsauces uz atcelto direktīvu uzskata par atsaucēm uz šo regulu.

51. pants

Pārejas pasākumi

1. Drošas paraksta radīšanas ierīces, kuru atbilstība noteikta saskaņā ar Direktīvas 1999/93/EK 3. panta 4. punktu, uzskata par kvalificētām elektroniskā paraksta radīšanas ierīcēm saskaņā ar šo regulu.

2. Kvalificētus sertifikātus, kas izsniegti fiziskām personām saskaņā ar Direktīvu 1999/93/EK, saskaņā ar šo regulu uzskata par kvalificētiem elektroniskā paraksta sertifikātiem līdz to derīguma termiņa beigām.

3. Sertificēšanas pakalpojuma sniedzējs, kas izsniedz kvalificētus sertifikātus saskaņā ar Direktīvu 1999/93/EK, cik vien iespējams drīz, bet ne vēlāk kā 2017. gada 1. jūlijā uzraudzības iestādei iesniedz atbilstības novērtēšanas ziņojumu. Līdz šāda atbilstības novērtēšanas ziņojuma iesniegšanai un brīdim, kad uzraudzības iestāde ir beigusi to izskatīt, minēto sertificēšanas pakalpojuma sniedzēju uzskata par kvalificētu uzticamības pakalpojumu sniedzēju saskaņā ar šo regulu.

4. Ja sertificēšanas pakalpojuma sniedzējs, kas izsniedz kvalificētus sertifikātus saskaņā ar Direktīvu 1999/93/EK, 3. punktā minētajā termiņā neiesniedz atbilstības novērtēšanas ziņojumu uzraudzības iestādei, minēto sertificēšanas pakalpojuma sniedzēju neuzskata par kvalificētu uzticamības pakalpojumu sniedzēju saskaņā ar šo regulu no 2017. gada 2. jūlija.

52. pants

Stāšanās spēkā

1. Šī regula stājas spēkā divdesmitajā dienā pēc tās publicēšanas *Eiropas Savienības Oficiālajā Vēstnesī*.

2. Šo regulu piemēro no 2016. gada 1. jūlija, izņemot:

a) 8. panta 3. punktu, 9. panta 5. punktu, 12. panta 2. līdz 9. punktu, 17. panta 8. punktu, 19. panta 4. punktu, 20. panta 4. punktu, 21. panta 4. punktu, 22. panta 5. punktu, 23. panta 3. punktu, 24. panta 5. punktu, 27. panta 4. un 5. punktu, 28. panta 6. punktu, 29. panta 2. punktu, 30. panta 3. un 4. punktu, 31. panta 3. punktu, 32. panta 3. punktu, 33. panta 2. punktu, 34. panta 2. punktu, 37. panta 4. un 5. punktu, 38. panta 6. punktu, 42. panta 2. punktu, 44. panta 2. punktu, 45. panta 2. punktu, 47. un 48. pantu, kurus piemēro no 2014. gada 17. septembra;

b) 7. pantu, 8. panta 1. un 2. punktu, 9., 10. un 11. pantu un 12. panta 1. punktu, kurus piemēro no dienas, kad sāk piemērot 8. panta 3. punktā un 12. panta 8. punktā minētos īstenošanas aktus;

c) 6. pantu, ko piemēro, sākot no dienas, kad ir pagājuši trīs gadi kopš 8. panta 3. punktā un 12. panta 8. punktā minēto īstenošanas aktu piemērošanas dienas.

3. Ja sarakstā, ko Komisija atbilstīgi 9. pantam ir publicējusi pirms šā panta 2. punkta c) apakšpunktā minētās dienas, ir iekļauta paziņotā elektroniskās identifikācijas shēma, tad elektroniskās identifikācijas līdzekļu atzīšana atbilstoši minētajai shēmai saskaņā ar 6. pantu notiek ne vēlāk kā 12 mēnešus pēc minētās shēmas publicēšanas, bet ne ātrāk par dienu, kas minēta šā panta 2. punkta c) apakšpunktā.

4. Neatkarīgi no šā panta 2. punkta c) apakšpunkta dalībvalsts var pieņemt lēmumu, ka elektroniskās identifikācijas shēmai atbilstoši elektroniskās identifikācijas līdzekļi, par ko saskaņā ar 9. panta 1. punktu ir paziņojusi kāda cita dalībvalsts, pirmajā minētajā dalībvalstī tiek atzīti no dienas, kad tiek piemēroti 8. panta 3. punktā un 12. panta 8. punktā minētie īstenošanas akti. Attiecīgās dalībvalstis informē Komisiju. Komisija šo informāciju publisko.

Šī regula uzliek saistības kopumā un ir tieši piemērojama visās dalībvalstīs.

Briselē, 2014. gada 23. jūlijā

Parlamenta vārdā –	*Padomes vārdā –*
priekšsēdētājs	*priekšsēdētājs*
M. SCHULZ	S. GOZI

I PIELIKUMS

PRASĪBAS KVALIFICĒTIEM ELEKTRONISKĀ PARAKSTA SERTIFIKĀTIEM

Kvalificēti elektroniskā paraksta sertifikāti ietver:

a) norādi, vismaz automatizētai apstrādei piemērotā formātā, par to, ka sertifikāts izsniegts kā kvalificēts elektroniskā paraksta sertifikāts;

b) tādu datu kopumu, kas nepārprotami apliecina tā kvalificētā uzticamības pakalpojumu sniedzēja identitāti, kurš izsniedz kvalificētos sertifikātus, ietverot vismaz informāciju par dalībvalsti, kurā pakalpojumu sniedzējs ir reģistrēts, un:

— juridiskai personai – nosaukumu un attiecīgā gadījumā reģistrācijas numuru atbilstīgi oficiālos reģistros norādītajai informācijai,

— fiziskai personai – personas vārdu;

c) vismaz parakstītāja vārdu vai pseidonīmu; ja izmanto pseidonīmu, to skaidri norāda;

d) elektroniskā paraksta validācijas datus, kas atbilst elektroniskā paraksta radīšanas datiem;

e) precīzu informāciju par sertifikāta derīguma termiņa sākumu un beigām;

f) sertifikāta identifikācijas kodu, kam jābūt kā kvalificētā uzticamības pakalpojumu sniedzēja unikālam kodam;

g) tā kvalificētā uzticamības pakalpojumu sniedzēja uzlaboto elektronisko parakstu vai uzlaboto elektronisko zīmogu, kurš izsniedz sertifikātu;

h) vietu, kur bez maksas pieejams sertifikāts, kas apliecina g) punktā minēto uzlaboto elektronisko parakstu vai uzlaboto elektronisko zīmogu;

i) vietu, kur pieejami pakalpojumi, ko var izmantot, lai noskaidrotu kvalificētā sertifikāta derīguma statusu;

j) ja elektroniskā paraksta radīšanas dati, kas saistīti ar elektroniskā paraksta validācijas datiem, atrodas kvalificētā elektroniskā paraksta radīšanas ierīcē – atbilstīgu norādi vismaz automatizētai apstrādei piemērotā formātā.

II PIELIKUMS

PRASĪBAS KVALIFICĒTĀM ELEKTRONISKĀ PARAKSTA RADĪŠANAS IERĪCĒM

1. Ar kvalificētām elektroniskā paraksta radīšanas ierīcēm, izmantojot atbilstīgus tehniskos un procesuālos līdzekļus, nodrošina vismaz to, ka:

   a) ir samērīgi nodrošināta elektroniskā paraksta radīšanā izmantoto elektroniskā paraksta radīšanas datu konfidencialitāte;

   b) elektroniskā paraksta radīšanā izmantotie elektroniskā paraksta radīšanas dati var praktiski parādīties tikai vienu reizi;

   c) ir pietiekama pārliecība par to, ka elektroniskā paraksta radīšanā izmantotos elektroniskā paraksta radīšanas datus nevar izgūt un elektroniskais paraksts ir uzticami aizsargāts pret viltošanu, izmantojot patlaban pieejamās tehnoloģijas;

   d) elektroniskā paraksta radīšanā izmantotos elektroniskā paraksta radīšanas datus likumīgais parakstītājs var droši aizsargāt pret to, ka tos izmanto citi.

2. Kvalificētās elektroniskā paraksta radīšanas ierīces nemaina parakstāmos datus vai nekavē šo datu parādīšanu parakstītājam pirms parakstīšanas.

3. Elektroniskā paraksta radīšanas datus parakstītāja vārdā var radīt vai pārvaldīt tikai kvalificēts uzticamības pakalpojumu sniedzējs.

4. Neskarot 1. punkta d) apakšpunktu, kvalificēti uzticamības pakalpojumu sniedzēji, kuri pārvalda elektroniskā paraksta radīšanas datus, parakstītāja vārdā var nokopēt elektroniskā paraksta radīšanas datus tikai rezerves kopijas izveides nolūkā, ja ir ievērotas šādas prasības:

   a) nokopēto datu kopu drošības līmenim jābūt tādam pašam, kāds tas ir oriģinālajām datu kopām;

   b) nokopēto datu kopu skaits nedrīkst pārsniegt minimālo skaitu, kāds nepieciešams, lai nodrošinātu pakalpojumu nepārtrauktību.

III PIELIKUMS

PRASĪBAS KVALIFICĒTIEM ELEKTRONISKO ZĪMOGU SERTIFIKĀTIEM

Kvalificēti elektronisko zīmogu sertifikāti ietver:

a) norādi, vismaz automatizētai apstrādei piemērotā formātā, par to, ka sertifikāts izsniegts kā kvalificēts elektroniskā zīmoga sertifikāts;

b) tādu datu kopumu, kas nepārprotami apliecina tā kvalificētā uzticamības pakalpojumu sniedzēja identitāti, kurš izsniedz kvalificētos sertifikātus, ietverot vismaz informāciju par dalībvalsti, kurā pakalpojumu sniedzējs ir reģistrēts, un:

— juridiskai personai – nosaukumu un attiecīgā gadījumā reģistrācijas numuru atbilstīgi oficiālos reģistros norādītajai informācijai,

— fiziskai personai – personas vārdu;

c) vismaz zīmoga radītāja vārdu un attiecīgā gadījumā reģistrācijas numuru atbilstīgi oficiālos reģistros norādītajai informācijai;

d) elektroniskā zīmoga validācijas datus, kas atbilst elektroniskā zīmoga radīšanas datiem;

e) precīzu informāciju par sertifikāta derīguma termiņa sākumu un beigām;

f) sertifikāta identifikācijas kodu, kam jābūt kā kvalificētā uzticamības pakalpojumu sniedzēja unikālam kodam;

g) tā kvalificētā uzticamības pakalpojumu sniedzēja uzlaboto elektronisko parakstu vai uzlaboto elektronisko zīmogu, kurš izsniedz sertifikātu;

h) vietu, kur bez maksas pieejams sertifikāts, kas apliecina g) punktā minēto uzlaboto elektronisko parakstu vai uzlaboto elektronisko zīmogu;

i) vietu, kur pieejami pakalpojumi, ko var izmantot, lai noskaidrotu kvalificētā sertifikāta derīguma statusu;

j) ja elektroniskā zīmoga radīšanas dati, kas saistīti ar elektroniskā zīmoga validācijas datiem, atrodas kvalificētā elektroniskā zīmoga radīšanas ierīcē – atbilstīgu norādi vismaz automatizētai apstrādei piemērotā formātā.

IV PIELIKUMS

PRASĪBAS KVALIFICĒTIEM TĪMEKĻA VIETŅU AUTENTIFIKĀCIJAS SERTIFIKĀTIEM

Kvalificēti tīmekļa vietņu autentifikācijas sertifikāti ietver:

a) norādi, vismaz automatizētai apstrādei piemērotā formātā, par to, ka sertifikāts izsniegts kā kvalificēts tīmekļa vietņu autentifikācijas sertifikāts;

b) tādu datu kopumu, kas nepārprotami apliecina tā kvalificētā uzticamības pakalpojumu sniedzēja identitāti, kurš izsniedz kvalificētos sertifikātus, ietverot vismaz informāciju par dalībvalsti, kurā pakalpojumu sniedzējs veic uzņēmējdarbību, un:

— juridiskai personai – nosaukumu un attiecīgā gadījumā reģistrācijas numuru atbilstīgi oficiālos reģistros norādītajai informācijai,

— fiziskai personai – personas vārdu;

c) fiziskai personai – vismaz tās personas vārdu vai pseidonīmu, kurai sertifikāts ir izsniegts. Ja tiek izmantots pseidonīms, to skaidri norāda;

juridiskai personai – vismaz tās juridiskās personas nosaukumu, kurai sertifikāts ir izdots, un attiecīgā gadījumā reģistrācijas numuru, kāds ir norādīts oficiālos reģistros;

d) tās fiziskās vai juridiskās personas adreses elementus (norādot vismaz pilsētu un valsti), kurai izsniegts sertifikāts, un attiecīgos gadījumos tā, kā norādīts oficiālos reģistros;

e) domēna vārdu vai vārdus, ko izmanto fiziskā vai juridiskā persona, kurai izsniegts sertifikāts;

f) precīzu informāciju par sertifikāta derīguma termiņa sākumu un beigām;

g) sertifikāta identifikācijas kodu, kam jābūt kā kvalificētā uzticamības pakalpojumu sniedzēja unikālam kodam;

h) tā kvalificētā uzticamības pakalpojumu sniedzēja uzlaboto elektronisko parakstu vai uzlaboto elektronisko zīmogu, kurš izsniedz sertifikātu;

i) vietu, kur bez maksas pieejams sertifikāts, kas apliecina h) punktā minēto uzlaboto elektronisko parakstu vai uzlaboto elektronisko zīmogu;

j) vietu, kur pieejami ar sertifikāta derīguma statusu saistīti pakalpojumi, ko var izmantot, lai noskaidrotu kvalificētā sertifikāta derīguma statusu.